

NAVAL WAR COLLEGE
Newport, R.I.

AN ANALYSIS OF
THE IMPACT OF NETWORK-CENTRIC WARFARE
ON THE DOCTRINE AND TACTICS, TECHNIQUES AND PROCEDURES
OF INTELLIGENCE AT THE OPERATIONAL LEVEL

By

Lieutenant Colonel Charles Harvey

Lieutenant Colonel Lance Schultz

United States Air Force

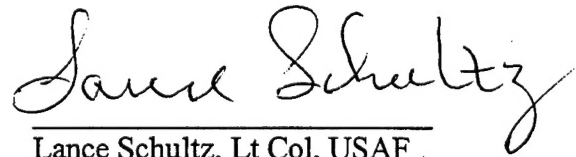
As an Advanced Research Project

A paper submitted to the Director of the Advanced Research Department in the Center for Naval Warfare Studies in partial satisfaction of the requirements for the Master of Arts Degree in National Security and Strategic Studies.

The Contents of this paper reflect our own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signatures: _____

Charles Harvey, Lt Col, USAF



Lance Schultz, Lt Col, USAF

1 June 1999

Faculty Advisors: _____

Virginia Baker, Lt Col, USAF

Roger Barnett, Professor

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority: N/A			
3. Declassification/Downgrading Schedule: N/A			
4. Distribution/Availability of Report: UNLIMITED			
5. Name of Performing Organization: ADVANCED RESEARCH DEPARTMENT			
6. Office Symbol: 35		7. Address: NAVAL WAR COLLEGE, 686 CUSHING RD., NEWPORT, RI 02841-5010	
8. Title (include Security Classification): An Analysis of the Impact of Network-Centric Warfare on the Doctrine and Tactics, Techniques and Procedures of Intelligence at the Operational Level			
9. Personal Authors: LtCol Charles Harvey, USAF and LtCol Lance Shultz, USAF			
10. Type of Report: Final		11. Date of Report: 1 June 1999	
12. Page Count: 72			
13. Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Advanced Research. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.			
14. Ten key words that relate to your paper: network-centric warfare (NCW), intelligence, Desert Fox, Joint Intelligence Doctrine			
15. Abstract: This project sought to determine the impacts of network-centric warfare (NCW) on the planning and direction of intelligence at the operational level, and what changes in joint intelligence doctrine (JID) and tactics, techniques, and procedures (TTPs) should/should not be made to support it? To meet those objectives, the analysis compared the NCW concept to the fundamentals upon which intelligence is to be employed in military operations (intelligence doctrine), the plans for taking doctrine to the field (the TTPs), and how the TTPs become reality in a real-world operation (DESERT FOX). To serve as a point of departure, a working model for NCW was established from the current literature. (This paper has classified appendices)			
16. Distribution / Availability of Abstract: A	Unclassified	Same As Rpt	DTIC Users
18. Abstract Security Classification: UNCLASSIFIED			
19. Name of Responsible Individual: Director, Advanced Research Department			
20. Telephone: (401) 841-2101		21. Office Symbol: 35	

ABSTRACT

This project sought to determine the impacts of network-centric warfare (NCW) on the planning and direction of intelligence at the operational level, and what changes in joint intelligence doctrine (JID) and tactics, techniques, and procedures (TTPs) should/should not be made to support it? To meet those objectives, the analysis compared the NCW concept to the fundamentals upon which intelligence is to be employed in military operations (intelligence doctrine), the plans for taking doctrine to the field (the TTPs), and how the TTPs become reality in a real-world operation (DESERT FOX). To serve as a point of departure, a working model for NCW was established from the current literature.

The NCW concept is still evolving. Enabled by the information management and networking technologies developed by the commercial world, NCW seeks to electronically link (through an information grid) the operational force (collectively, the shooter grid) to the various sensors capable of providing increased battlespace awareness (the sensor grid). With enhanced command and control, NCW intends to improve speed of command and enable self-synchronization as a means for achieving information dominance, the foundation for Joint Vision 2010.

Per the JID, intelligence is the responsibility of the commander, and is the means of providing not only the view of the battlespace, but the insight, perspective, and background necessary to understand the view. It is critical for determining objectives and developing courses of action for achieving them. Planning and directing are the keys to providing the required intelligence support, for they established the capability, and determine resource allocation and the priority for all subsequent actions in the intelligence cycle. By its very nature, intelligence will perhaps gain the most from the NCW concept.

In practice, intelligence is already incorporating many of fundamentals of NCW. As one would expect, the process of changing the doctrine is necessarily slow, but change is underway. Similarly, while the TTPs describe intended operations bounded by the current technology and common practice, they too reflect the fielding and integration of many of the NCW fundamentals, with sensor-to-shooter, the common operational picture, and reach-back the most visible applications. A similar state existed in DESERT FOX.

Continued evolution of both the DOD and the NCW concept will demand changes in intelligence discipline, asset, and task management. Resource allocation (along with location) and tasking authority, funding, security, and data management responsibilities and practices must all be adjusted accordingly. Communications will become increasingly critical. What must not be lost is the primacy of the commander, and the need to maintain management authority, responsibility, and accountability as the new technology is fielded.

To promote a smooth transition, additional research is needed to determine the impact of NCW on: the management of intelligence assets, the intelligence tasking mechanism, the characterization of the battlespace, the data architecture and the maintenance of its component parts, communications, security, training and required skills, and funding.

TABLE OF CONTENTS

ABSTRACT	<i>ii</i>
LIST OF ILLUSTRATIONS	<i>v</i>
INTRODUCTION	1
RESEARCH OVERVIEW	3
DEFINITIONS	5
Network Centric Warfare	5
Intelligence	11
ANALYSIS OF THE JOINT INTELLIGENCE DOCTRINE	20
Practical Realities	20
Analytical Methodology	23
Analytical Findings	24
Discipline Management	24
Asset Management	33
Task Management	41
Conclusions	44
RESEARCH CONCLUSIONS	47
RECOMMENDATIONS	51
BIBLIOGRAPHY	55
APPENDIX A AN ANALYSIS OF THE APPLICATION OF NCW PRINCIPLES TO THE TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) OF U.S. CENTRAL COMMAND (USCENTCOM) AND U.S. FORCES KOREA (USFK)	A-1
APPENDIX B AN ANALYSIS OF THE APPLICATION OF NCW PRINCIPLES IN OPERATION DESERT FOX	B-1

Appendices are stored separately due to classification.

LIST OF ILLUSTRATIONS

Figure 1	The Grid	6
Figure 2	Logical Model for Network-Centric Warfare	7
Figure 3	The Intelligence Cycle	15
Figure 4	Intelligence Planning and Direction Functions	16
Figure 5	General Military Intelligence Concerns	17

INTRODUCTION

Preparing for the challenges of the 21st Century: identifying the threats; developing and operationalizing new doctrine and tactics, techniques, and procedures (TTPs); and developing and integrating the new technology necessary to keep pace with potential adversaries is a daunting task. General Shelton, Chairman of the U.S. Joint Chiefs of Staff (JCS), speaking at the Marine Corps University on 10 February 1998 provided the following perspective and words of caution regarding technology:

Fanned by the ancient flames of ethnic, religious, cultural, and economic rivalry, many groups will challenge us at home and abroad. However, unlike past eras, terrorist groups and other nonstate actors will have access to state-of-the-art technology. They will have secure communications and access to global positioning satellites; highly advanced computer technology; and, perhaps most frightening of all, weapons of mass destruction.

But in thinking about the future, there is a key error we must avoid. *We must never fall into the trap of thinking that simply by fielding new and better systems we will maintain our lead.* History has taught us over and over again that *technology alone is not the answer.* The quality of our people, the caliber of our leaders, and *the operational concepts and doctrine we use to employ technology on the battlefield-they are the decisive factors.*¹
[emphasis added]

As the United States embarks on what has been described as the information wave “. . . characterized . . . by digitization, computers, and information technologies[,] . . . in which wars will be waged for control of data, information, and knowledge assets,”² it is critically important to review, validate, and update as required the doctrine and TTPs that define how America will conduct military operations in this new environment.

Joint Vision 2010 charts the course for transitioning America's military into the 21st

¹ General Henry H. Shelton, Adapted from 10 February 1998 Remarks at the Marine Corps University, Reprinted in “Operationalizing Joint Vision 2010,” Airpower Journal, vol. XII, no. 3, Fall 1998, 103-104.

² Ryan Henry and C. Edward Peartree, “Military Theory and Information Warfare,” Parameters, U.S. Army War College Quarterly, vol. XXVIII, no. 3, Autumn 1998, 122-123.

Century, wherein information management and networks become increasingly important to successful military operations. The vision serves as a guide for "... channeling ... people and leverag[ing] technological opportunities to achieve new levels of effectiveness in joint warfighting[, and] ... dominance across the range of military operations through the application of new operational concepts[, and by applying] ... unique [Service] capabilities within a joint framework of doctrine ...".³ Information superiority ("the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same") is the key enabler of the vision.⁴ Its measure of effectiveness is the ability to get the "... right information from the right sources to the right people at the right time in the right format."⁵ Success can only be achieved through integrated (read-networked) command, control, communications, computers (C⁴), and intelligence, surveillance, and reconnaissance (ISR) assets and capabilities.

The DOD is actively pursuing the objectives outlined in JV 2010. Earlier this year, Dr. F. Barry Horton, III, then Principal Deputy Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C³I), described the imperatives of JV 2010 as "... required by operational context; forced by resource constraints; motivated by organizational concerns; demanded by human limitations; and enabled by technology advances."⁶ At the same time, allies and potential coalition partners must also be considered. Re-emphasizing the concerns of General Shelton, it is not enough to consider technological solutions in isolation when doctrine and policy issues lie at the heart of these cooperative

³ Joint Chiefs of Staff, Joint Vision 2010 (Washington, D.C. : 1996), 1.

⁴ *Ibid.*, 16-17.

⁵ Arthur L. Money, "Statement," U.S. Congress, House, Armed Services Committee, Hearings before the House Armed Services Committee, 106th Cong, 23 February 1999, 1.
<<http://www.house.gov/hasc/testimony/106thcongress/99-02-23money.html>> (24 March 1999).

⁶ F. Barry Horton, III, quoted in Clarence A. Robinson, Jr., "Redundancy, Robustness Protect Vital National Information Links," SIGNAL Information Warfare Series, 1999, 2.

engagements⁷ and at the core of JV 2010. Clearly, this information wave presents opportunities; at the same time, there are numerous challenges to overcome before they can be realized.

In 1997, the National Defense Panel (NDP) charged the DOD to: “exploit information technology to integrate forces and platforms more effectively; accelerate network-centric operations linking sensors and weapons; and rely more heavily on distributed and networked battle fleets [which has application to all of the services].”⁸ These concepts are the heart of JV 2010, and at the same time, central to the evolving operational construct called network-centric warfare (NCW). Both NCW and intelligence are detailed later in the paper. Suffice it to say here, that intelligence is the discipline charged with providing the requisite information to support both the setting of national policy objectives and military operations. Communications (the backbone of the information grid) is the enabler for getting that information into the hands of the decision-maker or operational people in time for it to affect military operations in a positive manner. The evolving NCW construct, the operations-intelligence relationship within it, and the changes network-centrism may cause within intelligence proper are the focus of this paper.

RESEARCH OVERVIEW

This research was based on the hypothesis that the potential technology baseline and TTPs of NCW will have an impact on the planning and direction of intelligence at the operational level as defined in the existing joint intelligence doctrine (JID) and TTPs. The effort addressed the following question:

⁷ Lieutenant General John L. Woodward, “Statement,” U.S. Congress, House, Armed Services Committee, Hearings before the House Armed Services Committee, 106th Cong, 23 February 1999, 3.
<<http://www.house.gov/hasc/testimony/106thcongress/99-02-23woodward.html>> (24 March 1999).

⁸ Leslie West, “Exploiting the Information Revolution,” Sea Power, vol. 41, no. 3, March 1998, 38.

What are the impacts of network-centric warfare (NCW) on the planning and direction of intelligence at the operational level, and what changes in joint intelligence doctrine and TTPs should or should not be made to support it?

The research was based on the following observations:

1. TTPs establish the inter-discipline relationships and help define communications requirements.
2. Current doctrine is platform-centric.
3. Existing intelligence doctrine and TTPs do not address NCW requirements.
4. Existing technology baselines supporting intelligence do not provide NCW's requisite data warehouses, connectivity, or throughput.

Its objectives were to:

1. Advance NCW concept development.
2. Recommend changes to existing joint intelligence doctrine and TTPs.
3. Contribute to long-range planning, system development efforts, and acquisition strategy development.
4. Provide a foundation for additional research.

To achieve these objectives, the paper first establishes definitional foundations for NCW and intelligence that serve as the basis for the subsequent analysis. The analysis itself compares the existing JID and select TTPs to the perceived requirements of NCW. The paper then shifts perspective and examines the potential application of NCW concepts in a real-world operation, and ends with conclusions and recommendations. The definitional foundations for NCW and intelligence are meant to provide a common point of reference for the analysis. It is hoped that the results of the research would further the evolution of both.

In an effort to provide breadth and scope, yet keep the analysis within manageable limits, the intelligence TTPs from Central Command (CENTCOM) and U.S. Forces Korea (USFK) were selected. The real-world operation used to examine the state of NCW today as it relates to the planning and direction of intelligence was Operation DESERT FOX, the 1998 coalition operation in Iraq.

DEFINITIONS

NETWORK-CENTRIC WARFARE

NCW is a concept that is still evolving. Flowing from what Admiral Owens, former Vice Chairman JCS, called a system-of-systems approach to operations, it is now described in various forums as the latest revolution in military affairs (RMA), simply network-assisted warfare, or as nothing more than the latest fad. The description, or point of reference, presented here is drawn from existing literature, and attempts to capture the middle ground. It is meant to serve as a point of departure for the subsequent analysis.

Riding the wave of information technology embraced by the commercial world, the DOD is pursuing capabilities necessary to achieve information dominance. This effort is exemplified by an increased focus on networking in which the individual segments are viewed as part of an interactive whole, which is collectively driven by strategic choices.⁹ Within the DOD, increased connectivity and integration of C⁴ISR capabilities is designed to produce a robust multi-sensor information grid capable of providing dominant battlespace awareness. Through employment of advanced battle management techniques, the Department seeks to enable globally deployed forces to react faster and more efficiently than

⁹ Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, vol. 124/1/1,139, January 1998, 29.

potential adversaries.¹⁰ This concept is depicted in Figure 1, drawn from Joint Publication 6.0, Doctrine for C⁴ Systems Support to Joint Operations.

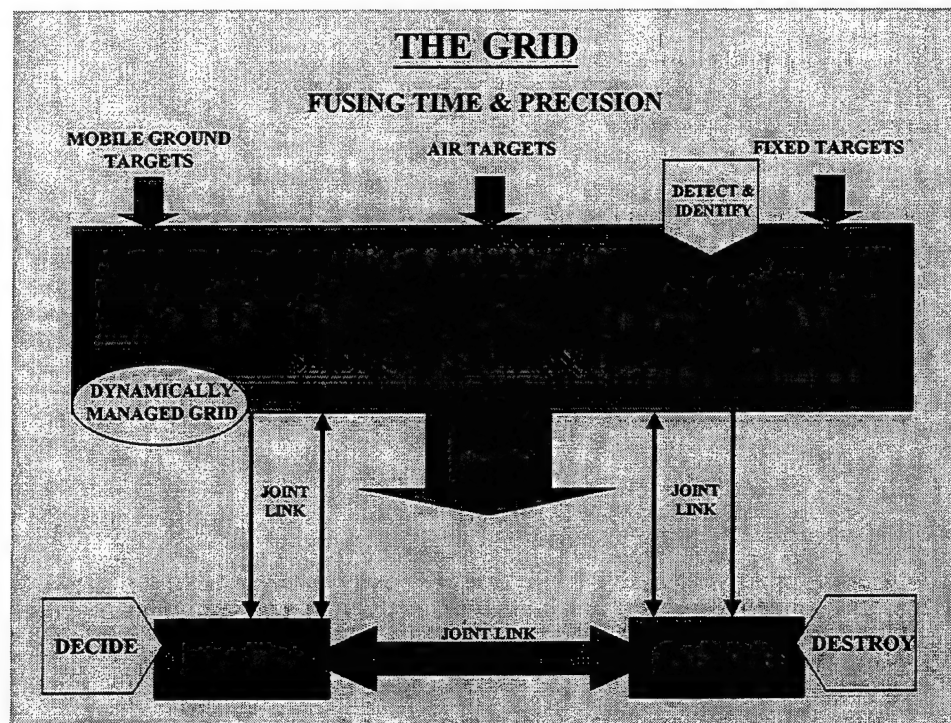


Figure 1: The Grid¹¹

Admiral Cebrowski, now President of the Naval War College and one of its leading advocates, describes NCW as follows:

[It] derives its power from the strong networking of well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command-and-control (C²) processes—to include high-speed automated assignment of resources to need—and integrated sensor grids closely coupled in time to shooters and C² processes.¹²

¹⁰ West, 38.

¹¹ Joint Chiefs of Staff, *Doctrine for Command, Control, Communications, and Computer (C⁴) Systems Support to Joint Operations* (Joint Pub 6-0) (Washington, D.C.: 30 May 1995), II-12.

¹² Arthur K. Cebrowski, quoted in Leslie West, "Exploiting the Information Revolution," *Sea Power*, vol. 41, no. 3, March 1998, 40.

The concept is depicted in Figure 2. Its success depends on data integrity, authenticity, timeliness, and confidentiality, along with assured access to suitable communications.¹³ The details of the NCW concept are highlighted in the paragraphs that follow.

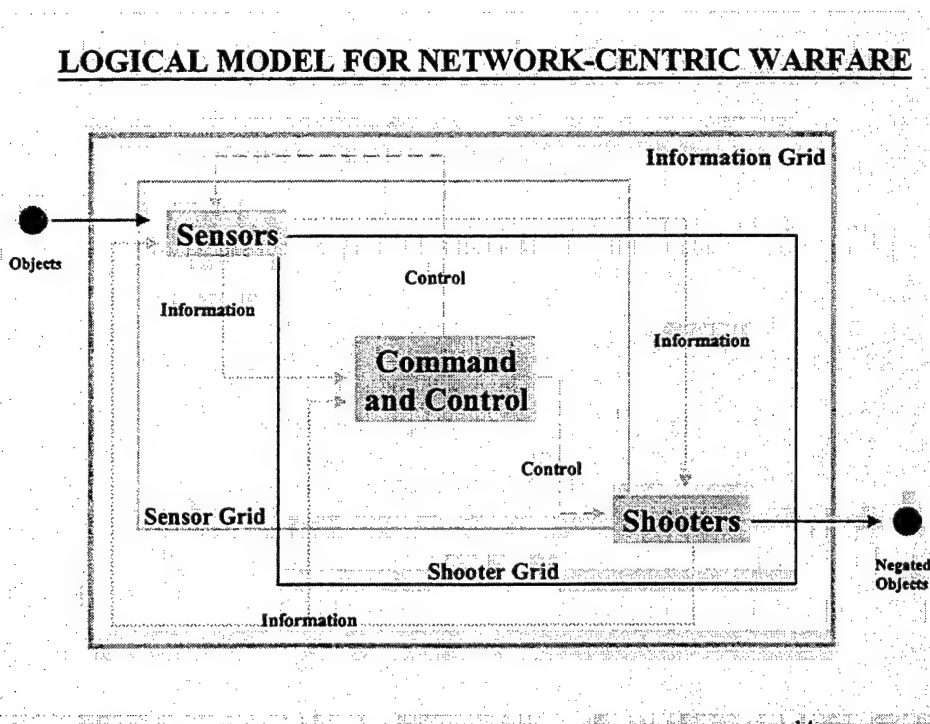


Figure 2: Logical Model for Network-Centric Warfare¹⁴

The ability to transport and process information is key to information superiority.¹⁵ The information grid includes the communications backbone that provides the essential connectivity and the data stores that house the available data, information, and intelligence. It also includes all of the computers and communications equipment along with the associated information management applications and operating systems used to manage this flow. Collectively, the information grid provides dial tone, web tone, and data tone for the

¹³ Dan Galik, "Defense in Depth: Security for Network-Centric Warfare," 2.
<http://www.chips.navy.mil/chips/archives/98_apr/galik.html> (12 February 1999).

¹⁴ Cebrowski and Gartska, 33.

¹⁵ Woodward, 2.

environment, and is the enabler for the sensor grid.¹⁶ In the DOD, the information grid is being implemented as the Global Information Grid under JCS auspices.¹⁷ In practice, the Global Information Grid is the combination of existing and planned communications capabilities.

The sensor grid provides the operational force its awareness, illuminating the sights, sounds, and perceptions of the battlespace. Its size and content are dictated by the demands of the operation; its parts are dynamically reconfigured to meet the specific mission tasking. It is composed of all of the available sensors, including those imbedded in others to monitor performance or consumables, and the application software that makes the sensors functional. Battlespace awareness is achieved through dynamic sensor tasking, the effective processing and fusion of the collected data into a usable form, and the timely distribution of the results to the consumer over the information grid.¹⁸

The engagement grid is a collection of systems or software algorithms designed to place data in the hands of a decision-maker in a format that enhances decision making. It is not designed to take the decision out of the hands of the commander, but improve his or her awareness of all of the factors that might influence their decisions, presenting them in a format that enhances their perspective and their options. Like the sensor grid, the engagement grid is dynamically tailored to the needs of the decision-maker and the demands of the operational environment. If effectively tailored and employed, the engagement grid

¹⁶ Joint Chiefs of Staff, "Observations on the Emergence of Network-Centric Warfare," J-6 Information Paper, 3. <<http://www.dtic.mil/jcs/j6/education/warfare.html>> (12 February 1999).

¹⁷ Woodward, 4.

¹⁸ Joint Chiefs of Staff, "Observations on the Emergence of Network-Centric Warfare," J-6 Information Paper, 4-6.

enables predictive planning and preemption; integrated force management; execution of time-critical missions; increased ops tempo, massed effects, and maximized combat power; and locks-out enemy courses of action (COAs) as a result.¹⁹

Collectively, the capabilities of the sensor, information, and engagement grids, when effectively employed, are designed to increase speed of command and the self-synchronization of the forces employed in the operation. Admiral Johnson, Chief of Naval Operations (CNO), describes speed of command as "the ability to rapidly collect information, assess the situation, develop a course of action, and immediately execute with overwhelming effect."²⁰ Providing the decision-maker with increased battlespace awareness in real- or near-real-time not only enhances the quality of decision, but also reduces the time required to make it. As a result, blue-force actions occur on a timeline that restricts (or locks-out) enemy alternatives.²¹

Self-synchronization is intended to minimize the amount of time taken to observe and orient within the OODA (observe, orient, decide, and act) Loop, and to increase the effective application of combat power. It demands a clear understanding of the decision-maker's intent, and access to the same information, though the amount displayed or interrogated may be tailored to support individual mission tasking. Given appropriate communications connectivity, self-synchronization occurs when authority is given to task-organize from the bottom-up in response to assigned tasking, and to dynamically reorient and synchronize actions in response to the ebb and flow of the battlespace, without command intervention.²²

¹⁹ Joint Chiefs of Staff, "Observations on the Emergence of Network-Centric Warfare," J-6 Information Paper, 6-7.

²⁰ Admiral Jay Johnson, quoted in Leslie West, "Exploiting the Information Revolution," Sea Power, vol. 41, no. 3, March 1998, 38.

²¹ Cebrowski and Gartska, 33.

²² *Ibid.*, 33-35.

Obviously, the operational Commander-In-Chief (CINC) or Joint Force Commander (JFC) must allow the assigned forces to self-synchronize, which is not prescribed in current operational TTPs. The forces themselves must have access to the information and engagement grids to obtain the requisite information upon which to base such decisions.

NCW promises several advantages over the current platform-centric concept employed today. Speed of command and self-synchronization together promise to shift the focus of warfare from attrition to one in which high ops tempo and rates of change lock out enemy alternatives while locking-in blue force success. In doing so, NCW can potentially "offset a disadvantage in numbers, technology, or position."²³

The U.S. Army's November 1997 Advanced Warfighting Exercise (AWE), in which network-centric concepts played an important part, suggests changes in the way operations are defined, from deep, close, and rear, to one based on time (current and future) or function (engagement or sustainment). As a result of the exercises, others concluded that the commander is more interested in accuracy and timeliness of the information than supporting analysis. If this is accepted, it further suggests opportunities for reducing the number of people on battlestaffs performing intelligence functions, and that battlestaffs be reorganized to focus on situational awareness and battlefield synchronization.²⁴

While the information revolution and its associated technologies offer many opportunities for improving the way DOD (and intelligence) does business, a prudent evolution of doctrine and TTPs based on a thorough analysis of existing capabilities and processes is warranted. The Honorable Arthur L. Money, ASD for C³I and DOD's Chief

²³ Ibid., 32.

²⁴ Stephen F. Garrett, "Evolving Information-Age Battle Staffs," Military Review, vol. LXXVIII, no. 2, March-April 1998, 28-36.

Information Officer (CIO), in testimony before the House Armed Services Committee, voiced concerns in speaking about security policy and business practices.

Information technology merely enforces and implements the decisions we program them to make. If we don't think through the problem and solution carefully, information technology will only provide us a bad answer faster. If we deny critical information to a coalition partner who is working with our forces, then we will have less defense. If we apply information technology to an inefficient business process, then we will have automated inefficiency. There are many natural tensions in the exploitation of information superiority, and we must be resolved to address these tensions as we employ the technology. We also must examine our security policies and determine what we need to protect and how best to protect it.²⁵

Lt Gen Woodward, the U.S. JCS's Director for C⁴ Systems, in testimony to the same committee, voiced his concerns in more operational terms, saying "... the process of transitioning to a network-centric force is just getting started ...". We must deal with a myriad of "... non-trivial technology, organizational, and doctrinal components associated with network-centric warfare, ... [and] that synchronizing the C⁴ systems and technology components required to enable a network-centric force is ... a daunting challenge."²⁶

The potential of NCW, its potential impact on intelligence, and the collective concerns of Secretary Money and Lt Gen Woodward, are central to the analysis of this research, which is summarized following the description of intelligence provided in the next section.

INTELLIGENCE

The intelligence community (IC) includes assets organic to the DOD, as well as those from the Central Intelligence Agency and the Departments of State, Energy, Justice, and

²⁵ Money, 6-7.

²⁶ Woodward, 4.

Treasury.²⁷ While the DOD manages a significant share of the government's intelligence resources and assets, and shoulders tremendous responsibilities in times of war, the diverse charters, resources, and missions of all of these agencies must be taken into account when discussing intelligence doctrine, TTPs, and specific intelligence support programs. Although "[e]ach agency is assigned clearly defined missions and areas of responsibility to minimize duplication of effort and questions over functional responsibilities,"²⁸ each has unique capabilities that result in a degree of overlap. For example, DOD resources may support counterdrug operations along the US borders and coastline, the principal domains of Immigration and Naturalization Service (INS) and the U.S. Coast Guard (USCG), respectively. In another case, the FBI, a domestic law enforcement agency, participated in the Khobar Towers bombing investigation in support of the DOD. At the operational level, interaction between the agencies in the IC and unity of effort in support of the JFC is essential.

Highlighting the distinction between data, information, and intelligence is important to the subsequent analysis of the impact of NCW on intelligence. Data, as defined in the intelligence discipline, is a "[r]epresentation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means[,or a]ny representations such as characters or analog quantities to which meaning is or might be assigned."²⁹ Data may or may not have any direct value to the operation. In fact, in its raw form, the sheer volume of data collected by some sources may simply overwhelm

²⁷ Joint Chiefs of Staff, National Intelligence Support to Joint Operations (Joint Pub 2-02) (Washington, D.C.: September 28, 1998), III-2

²⁸ *Ibid.*, I-3

²⁹ Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms (Joint Pub 1-02) (Washington, D.C.: March 23, 1994), 104.

communications systems, processors, intelligence analysts, and operators. However, by properly framing questions and targeting specific intelligence assets, the resultant data can have a direct impact on the application of military force. For example, a hardcopy print can be used to answer 'Is the bridge up or down?' and thereby support an immediate restrike decision without further processing or analysis.

Information is data that has been given a more tangible form through processing, or has been assigned a sense of meaning through analysis.³⁰ The current embryonic sensor-to-shooter applications provide examples of the direct application of information. A case in point: radar phase-history (data) is transformed into a series of literal images (information), one of which is transferred to an aircraft to support a strike option.

Data and information are the foundation for intelligence, which is "[t]he product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries [and] . . . [i]nformation and knowledge about an adversary obtained through observation, investigation, analysis, or understanding."³¹ In many cases, intelligence is based on intuition, and requires the fusion of disparate data points. As such, it is time consuming to produce but has significant operational value. Due to its complexity, it also introduces risk into the operational equation.

Within the intelligence community, data, information, and intelligence are generated from a wide variety of sources through different collection methods, and processing and production techniques. Collection platforms range from human sources to spaceborne sensors, while processing and production varies from mere transcription of hand-written notes to format changes accomplished by large computer complexes. Intelligence is

³⁰ Ibid., 184.

³¹ Ibid., 188.

characterized as counterintelligence (CI); human (HUMINT); imagery (IMINT); measurement and signature (MASINT); open source (OSINT); signals (SIGINT); and technical (TECHINT), dependent upon its sources, methods, and product.³²

Requests for intelligence support are levied as requirements, defined as “[a]ny subject, general or specific, upon which there is a need for the collection of [data or] information, or the production of intelligence.”³³ They are expressed in the form of requests for information (RFIs), production requests (PRs), or collection requests (CR). The former is a general statement of need that may be satisfied by the reevaluation or republication of current holdings. PRs require additional copies of things for which production tasking already exists. CRs mandate the acquisition of new data; the CR and resultant actions are managed through the collection management (CM) process. Fundamentally, all requests for support should begin as an RFI, but as tensions escalate, often take the form of CRs, which are more often than not, preceded by a request for a specific collector based on its inherent capabilities without regard to the specific question under consideration. Regardless of how the need is captured, the actions taken to satisfy any of the three are depicted in Figure 3, The Intelligence Cycle.³⁴

Planning and Directing is the key element in the intelligence cycle. The actions taken here define available assets, establish priorities, and authorize the expenditure of resources necessary to accomplish all of the other functions in the cycle. Planning and direction functions are highlighted in Figure 4. The nature of the original request will dictate what parts of the intelligence cycle actually respond to the request. In general, processing and

³² Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0) (Washington, D.C.: 5 May 95), II-1.

³³ Joint Chiefs of Staff, Joint Pub 1-02, 190.

³⁴ Joint Chiefs of Staff, Joint Pub 2-02, I-1-I-3.

exploitation generally turns data into a usable form, or converts it into information. Analysis and production generates more fused or finished information or intelligence. Evaluation and feedback is the customers' critique of the process; it is meant to ensure intelligence is responsive to their needs.

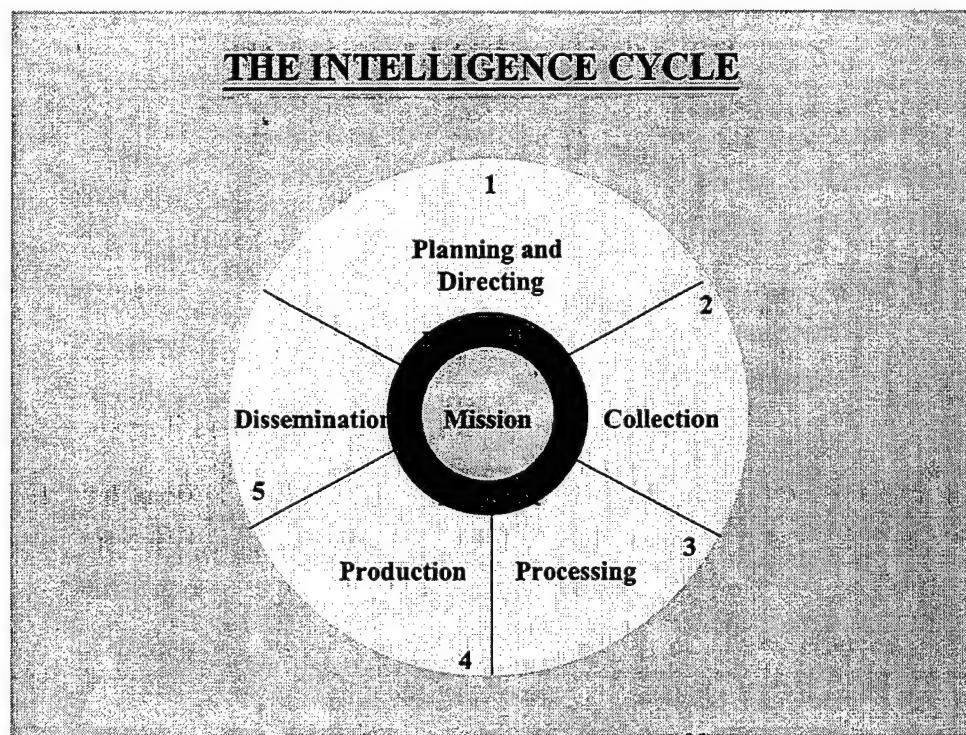


Figure 3: The Intelligence Cycle³⁵

Dissemination is the critical link to the consumer. "Push" and "pull" are terms that describe dissemination concepts. In the "push" concept, intelligence products are automatically transferred to the consumer based on predefined ground rules. In the "pull" concept, consumers must search for the answer to their question, accessing databases or other files to satisfy their requirements. Both options are very much communications dependent and security restricted.

³⁵ Joint Chiefs of Staff, Joint Pub 2-01, Figure III-1, III-2.

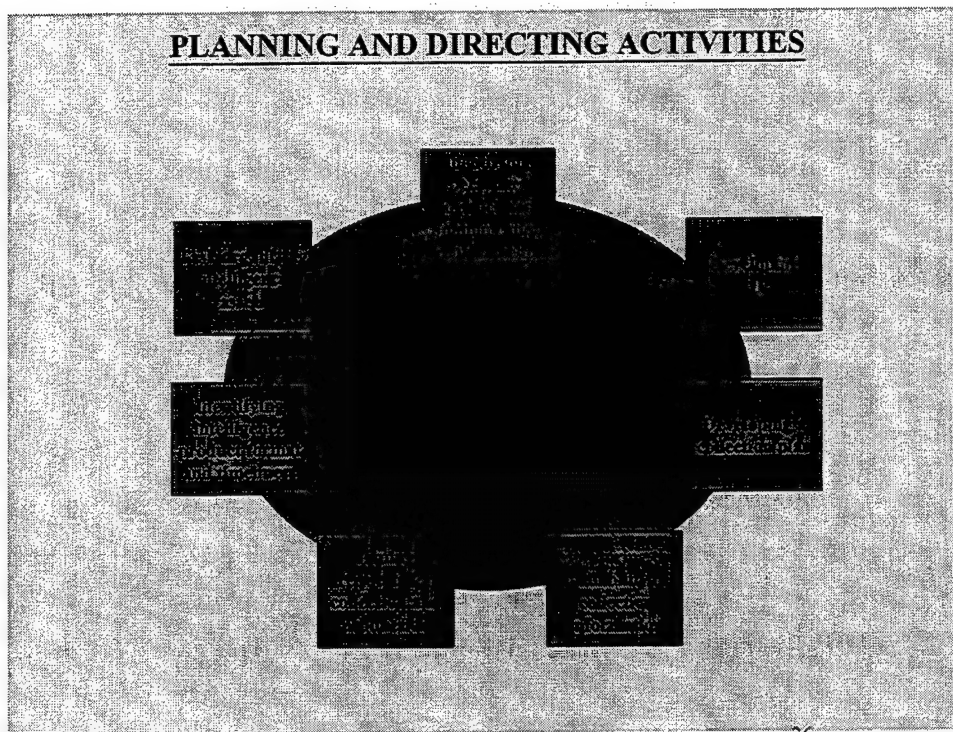


Figure 4: Planning and Directing Activities³⁶

The objective of the IC is to provide seamless support to national decision makers and the United States military, across the spectrum of conflict from peace to war. In peacetime, strategic intelligence "... is required for the formulation of strategy, policy, and military plans and operations at national and theater levels."³⁷ Figure 5 highlights the complexity of the environment and the factors derived from it by intelligence. These factors are used to determine the required size and capabilities of America's military, and are critical to any military operation. The reader should note that much of this information is derived by synthesizing disparate pieces of data, information, or intelligence based on insight and intuition.

Some of the greatest intelligence challenges lie in supporting military operations other than war (MOOTW). These operations are particularly problematic because of the

³⁶ Joint Chiefs of Staff, Joint Intelligence Support to Military Operations (Joint Pub 2-01) (Washington, D.C.: November 20, 1996), Figure III-2, III-3.

³⁷ Joint Chiefs of Staff, Joint Pub 2-0, II-1.

unique demands they place upon the IC and because “[t]here are no standard templates for structuring intelligence support to military operations other than war . . .”³⁸ American and allied military forces, often along with private volunteer or non-governmental organizations (PVO/NGO), operate within crosscurrents of political loyalties and divergent ethnic, cultural, and religious groups, all of which place unique demands on intelligence. A key observation from OPERATION JOINT ENDEAVOR is that “[c]ommanders need to gain a more complete understanding of the integrated operations/intelligence process and how to leverage intelligence in support of peace operations—the Information Age is forcing a paradigm shift . . . [and d]octrine, CONOPS, TTP, and IPB need to be adjusted [accordingly].”³⁹

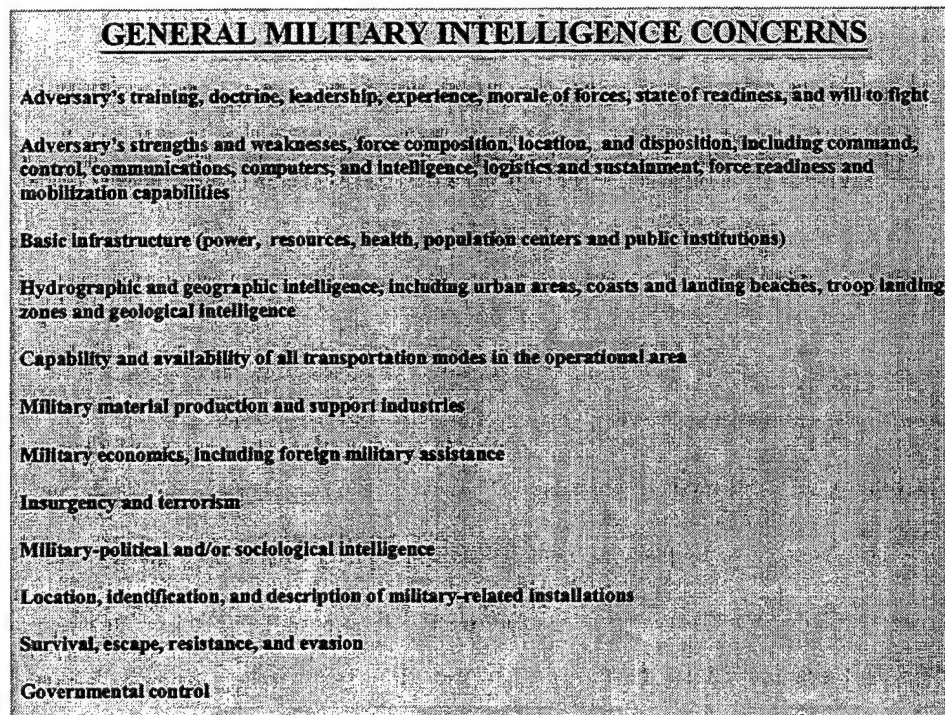


Figure 5: General Military Intelligence Concerns⁴⁰

³⁸ Joint Warfighting Center, Joint Task Force Commander's Handbook for Peace Operations (Fort Monroe, VA: 1995), 31.

³⁹ Larry Wentz, Lessons from Bosnia: the IFOR Experience (Washington, D.C.: 1997), 113.

⁴⁰ Joint Chiefs of Staff, Joint Pub 2-01, Figure 3-18, III-32.

Throughout the spectrum of conflict, “[t]he JFC [as the principal warfighter] depends on timely, accurate intelligence on an adversary’s strategy, tactics, intent, objectives, strengths, weaknesses, values, and critical vulnerabilities.”⁴¹ The basis for that support is established in both deliberate and crisis action planning. In addition to providing the foundation for the commander’s estimate, intelligence supports “. . . the development of alternative courses of action (COAs) . . . collecting and analyzing already existing [or new] information to produce intelligence on the adversary, terrain, meteorological and oceanographic (METOC) and geographic features that affect friendly and adversary forces through the joint intelligence preparation of the battlespace (JIPB) process.”⁴² With advances in information technology, the volume of available data, information, and intelligence is expanding dramatically, as is the ability to provide direct access to a broader base of consumers. What is lagging behind is the ability to correlate and fuse the data within ever decreasing operational timelines.

This is particularly evident in war, where even greater IC responsibilities and risks emerge. “The [overall] demand for intelligence support increases significantly [and] more intelligence personnel [are] needed in the AOR and/or JOA [area of responsibility/joint operations area] at all command levels.”⁴³ The intelligence required differs from echelon to echelon and serves many functions, including intelligence preparation of the battlefield, force application, and force protection. It must always be presented in a format acceptable to the user.⁴⁴ National level non-DOD intelligence support is coordinated by the JCS-J2; national

⁴¹ Ibid., III-1.

⁴² Ibid., II-2.

⁴³ Ibid., III-6.

⁴⁴ Ibid., III-7 and 8.

intelligence support teams (NIST) serve as the direct liaison between the operational CINC or JFC and the supporting agency.⁴⁵

Effective intelligence sharing also necessitates “. . . liaison between joint and multinational force intelligence structures . . . ”;⁴⁶ however, methods must be “established . . . to expedite sanitization and sharing of US-generated intelligence products . . . ”.⁴⁷ “National Disclosure Policy (NDP)-1 governs how the United States releases military information to foreign governments and international organizations and establishes eligibility criteria to receive releasable information.”⁴⁸ DIA coordinates foreign disclosure/release, while the JCS-J2 manages intelligence support requirements for operations conducted under the auspices of the UN.⁴⁹ Beyond these technical hurdles, some potential partners are less than comfortable dealing with the intelligence agencies of the major nations.⁵⁰

In total, intelligence is charged with providing the right data, information, or intelligence in time to have a positive affect on military operations. To have any value, much of that support demands the correlation and fusion of current holding, or the collection and subsequent correlation and fusion of new data or information. To fulfill that charter, the intelligence specialist must have access to both the CINC or JFC to clearly understand the operational objective, and to as much of the known data, information, and intelligence as possible to ensure timely tailored support.

⁴⁵ Joint Chiefs of Staff, Joint Pub 2-02, II-5.

⁴⁶ Joint Chiefs of Staff, Joint Pub 2-01, A-6.

⁴⁷ Ibid., A-6.

⁴⁸ Ibid., E-4.

⁴⁹ Ibid., II-6.

⁵⁰ Par Eriksson, “Intelligence in Peacekeeping Operations,” International Journal of Intelligence and Counterintelligence, vol. 10, no. 1, Spring 1997, 1 and 5.

ANALYSIS OF THE JOINT INTELLIGENCE DOCTRINE

PRACTICAL REALITIES

With the end of the Cold War, American interests shifted to domestic issues in which balancing the Federal budget became a priority. In constant Fiscal Year 00 dollars, defense spending declined from a peak in the mid-80's of \$430 billion to \$283 billion in 1999;⁵¹ intelligence and communications shared in that drawdown. Throughout the decline, the DOD followed a practical and resource conscious philosophy of doing more with less, but with an increased emphasis on efficiency and effectiveness.

As General Shelton indicated in the quote at the beginning of the paper, the world is still full of challenges to America's interests. The rise of non-state actors and issues, the increasing involvement in and growing complexity of MOOTW, and the threat of non-rational or non-state actors acquiring weapons of mass destruction all contribute to the complexity of the required intelligence. Further, intelligence must address issues far beyond a potential adversary's political-military capabilities--economics, geopolitics, political objectives, history, culture, philosophy, and technology are increasingly important.⁵² To be successful, the intelligence specialist must be intuitive and adept at analysis and problem solving.

America's move towards NCW is viewed by some as a logical extension of its culture. Its "... global interests and responsibilities provide the motivation; its success in

⁵¹ "Budgets," *Air Force Magazine*, vol. 82, no. 5, May 1999, 58.

⁵² Robert K. Ackerman, "Air Intelligence Confronts New Geopolitical Realities," *SIGNAL*, vol. 53, no. 2, October 1998, 27.

key information technologies, especially data networking, provide the potential.”⁵³ In pursuit of the objectives of JV 2010 from which NCW draws its foundation, the U.S. ASD for C³I, has established ten goals for the department. They include the fielding of a global networked information enterprise, fully integrated joint and combined C³ and ISR, the reinvention of intelligence, a new technology plan focused on commercial technology, and a knowledge-based work force.⁵⁴ All of the services have programs underway to improve their information infrastructure, and battlelabs to test new concepts, TTPs, and the fundamental assumptions of JV 2010.⁵⁵ By their nature, they also examine the fundamentals of NCW.

While the U.S. is far ahead of the rest of the world in addressing the opportunities afforded by information technology, the migration towards a network-centric environment presents significant challenges. New collection technologies and virtual access to data, information, or intelligence can simply overwhelm the consumer with the sheer volume of available material. Given the expanded access, the consumer now demands preprocessing or conversion of the holdings into a more readily usable form.⁵⁶ They also require improved search engines and distribution techniques, as shortened operational timelines preclude searching through every holding for a specific item or collection of information.⁵⁷ To truly satisfy operational requirements takes more than simple connectivity and access.

Developing, fielding, and operating JV 2010’s information infrastructure (NCW’s information grid and providing the connectivity cited above) must be approached

⁵³ David C. Gompert, Richard L. Kugler, and Martin C. Libicki, Mind the Gap, Promoting a Transatlantic Revolution in Military Affairs (Washington: National Defense University Press 1999), 3.

⁵⁴ Money, 3-5.

⁵⁵ Shelton, 2.

⁵⁶ Robert Callum, “Will Our Forces Match,” U.S. Naval Institute Proceedings, vol. 124/8/1,146, August 1998, 50.

⁵⁷ Susan M. Gordon, quoted by Clarence A. Robinson, Jr., “Intelligence Agency Adjusts as Mission Possible Unfolds,” SIGNAL, vol. 53, no. 2, October 1998, 18.

systematically. The U.S. JCS Director for C⁴ (JCS/J-6) acknowledges a wide range of deficiencies that must be addressed as part of the solution. They include: C⁴ interoperability, C⁴ force modernization, training, transmission capacity and information management, joint network management, base-level C⁴ infrastructure, information assurance, the technical workforce itself, and the acquisition process for buying and fielding C⁴ systems and capabilities.⁵⁸ At the same time, the department must overcome a lack of visibility into the development and fielding of the infrastructure.⁵⁹ So while the U.S. is in the forefront of the information wave, a lot of the infrastructure has not yet been fielded, and the effort necessary to accomplish it must compete for scarce defense resources.

While the U.S. is actively pursuing new information technologies and operational concepts necessary to take advantage of them, the same cannot be said of potential allies and partners, both of which will play a greater role in all future military operations across the spectrum of conflict. As late as 1997, an estimated half of the world's population had never made a phone call.⁶⁰ While that may be an oversimplification, it is true that America's acquisition and integration of information technologies is proceeding at a much faster pace than is even its NATO allies.⁶¹ As a result, American forces deployed elsewhere in the world will face difficulties in obtaining landing rights for satellite communications (approval to operate) and frequency authorizations (to avoid local spectrum interference), and a broad range of capabilities and weaknesses in the requisite local infrastructure in which they must

⁵⁸ Woodward, 6.

⁵⁹ Money, 5.

⁶⁰ Henry and Peartree, 132.

⁶¹ Gompert, Kugler, and Libicki, 4.

operate.⁶² These differences in capabilities will undoubtedly exacerbate interoperability and data sharing problems, both of which are key to the success of the NCW concept.

This is the backdrop against which the research was conducted. The U.S. is undoubtedly the leader in developing the new information technologies on which the NCW concept is based, and is far ahead of the rest of the world in integrating them and the operational concepts necessary to employ them effectively. However, promulgating the technology throughout the operational forces in a resource constrained environment and getting potential allies and coalition partners onboard, remains a challenge.

ANALYTICAL METHODOLOGY

The following publications detail the existing U.S. Joint Intelligence Doctrine and are the focus of this analysis.

Joint Publication 2-0	Joint Doctrine for Intelligence Support to Operations
Joint Publication 2-01	Joint Intelligence Support to Military Operations
Joint Publication 2-01.2	Joint Doctrine and TTP for Counterintelligence Support to Operations
Joint Publication 2-02	National Intelligence Support to Joint Operations

The draft publications listed below were included in the analysis only in so far as they reflect ongoing discussion within the DOD.

Joint Publication 2-01.1	JTTP for Intelligence Support to Targeting (Draft)
Joint Publication 2-01.3	JTTP for Joint Intelligence Preparation of Battlespace (Draft)
Joint Publication 2-03	JTTP for Geospatial Information and Services Support for Joint Operations (Draft)

⁶² Woodward, 3.

As one might expect, these publications document how to employ existing intelligence assets and capabilities. During the analysis, each of the intelligence publications listed above was compared to the requirements of NCW, or the opportunities it presents, outlined earlier in the paper, to determine mismatches, shortfalls, potential problems, and alternatives. Where appropriate, the analysis identified a recommended approach. As written, the pubs may not represent the ideal for intelligence in a NCW environment. In the paragraphs that follow, some issues are presented that call for change, and others that demand the status quo.

ANALYTICAL FINDINGS

Rather than a line in-line out scrub of each publication, the research evaluated the ability of the set as a whole to deal effectively with three issues identified as critical to the planning and direction of intelligence in a network-centric environment. The first issue looks at planning and direction from a discipline management perspective, and by default, the operations-intelligence relationship. The second examines asset management, in which the location of intelligence assets, resource allocation, and tasking authority are key considerations. The third issue delves into the actual intelligence tasking mechanism itself, or more specifically, how the consumer asks for support. In each, the planning and directing activities are highlighted by the required actions performed in accomplishing the overall category.

Discipline Management

In discipline management, the research focused on the potential for realigning the responsibilities of operations and intelligence to improve operational effectiveness in a network-centric environment. The development of sophisticated information management

applications combined with the fundamental concepts of NCW suggests an opportunity for change.

Per Joint Pub 2-0, "acquiring intelligence is the responsibility of the commander."⁶³ As the doctrine is written, the staff agent charged with executing that responsibility is the senior intelligence officer (operationally, the J-2). The underlying question is, given the access to data, information, and intelligence the information grid of NCW affords, what intelligence support is required, or does everyone or application acquire their or its own intelligence as part of a self-synchronization effort?

It is said the commander is the best intelligence officer,⁶⁴ for he or she determines the operational objectives and establishes the intelligence requirements. The commander (and operations in general) must guard against the philosophy "just give me the information (or access to it) and I'll decide" which the NCW concept may foster. The technology may allow it, but there are many factors, outlined in the following paragraphs, that mitigate against that approach.

In the purest form of NCW, sensor-to-shooter applications take data, information, or intelligence generated "automatically" by the sensor grid in response to a perceived operational need, move it through the information grid in real- or near-real-time, and apply it directly through the shooter grid to the military problem. All of this is potentially done without human intervention. In those cases where people are involved, consumers have an opportunity to become their own intelligence officers. With more sophisticated consumers comes increasing demands for direct access to the data stores,⁶⁵ and again, the information

⁶³ Joint Chiefs of Staff, Joint Pub 2-0, IV-3.

⁶⁴ Amos Kovacs, "The Nonuse of Intelligence," International Journal of Intelligence and Counterintelligence, vol. 10, no. 4, Winter 1997-1998, 406.

⁶⁵ Susan M. Gordon, quoted by Clarence A. Robinson, Jr., 19.

grid of NCW affords that opportunity. Ultimately, the commander must decide, based on operational requirements, security constraints, and available resources, who has access to what data, information, or intelligence, and for what purpose.

Looking closer at sensor-to-shooter applications reveals potential pitfalls that must be considered in the evolution of NCW. Imbedding an intelligence application or software algorithm within the weapon system itself, as is the case with high-speed anti-radiation missiles, reduces the decision cycle to seconds, given prior command execution authority. A variant of this theme is the common operational picture (COP). In this case, mission materials are sent directly to the potential consumer (sometimes bypassing the normal processing and production capabilities) and displayed automatically in a graphic representation of the battlespace. The decision-maker then acts without further assistance. In some cases, the decision-maker may be a shooter. Here again, the decision cycle is potentially reduced to seconds, though normally is significantly longer in that the consumer must sort through all of the material received to find the relevant data (or wait for it to appear), before passing the management decision on to the shooter for execution. Both of these are excellent examples of the advantages of network-centrism.

The COP is much more difficult to create when the operational picture requires complex data sets (i.e., multi- or hyper-spectral information and imagery), information developed by human sources, or the correlation and fusion of a combination of several data or information sources to obtain the right perspective. Security in these circumstances is also a bigger concern. Sensor-to-shooter applications are still possible, but involve a much more elaborate construct to properly frame the question prior to seeking an answer and a much

better understanding of the possible solution set before the process can be fully automated. The algorithms necessary for conducting these complex tasks aren't available.

While providing universal access to the information grid is technically feasible, it may not always be the best approach. When the question is well bounded and the answer involves a small set of data or information, consumers should have the option of doing their own analysis, given security constraints do not preclude it. While some redundancy has merit in the development of intelligence, duplication of effort, where several consumers search for the same data, information, or intelligence for the same reason, or similar products are produced by several organizations, must be minimized. In point of fact, the operational procedures necessary for operating in this type of an environment are still evolving.

With more complex operational questions, demanding larger or more complex data sets, or the fusion of information from multiple sources, the logic of an individual consumer taking this approach is highly suspect. Assuming the consumer has sufficient background and training with the systems involved and the issue in question, and access to all of the required information, and the right security authorization, there is the question of committing time and energy to the task. In today's environment, few people have neither the capacity nor a desire to take on work already being done by someone else.

For example, attacking a power grid may appear to be a straightforward targeting problem. Considering just the desired affect and the potential for unintended consequences from the many aspects of the problem, the task is much more complex. Though not all inclusive, determining what lies in the proximity of the target, the impact of the power loss, and the contribution the attack may have on the operation as a whole, are important aspects which cannot be developed without substantial effort. To develop the required targeting

package requires substantial training and a commitment of resources beyond the capability of the general consumer.

For the consumer, data interpretation, validity, and verification must also be considered. Direct access to the data stores makes the consumer responsible. They can either accept the data, information, or intelligence contained therein on face value, making the assumption that the information grid is impenetrable and failsafe, or verify and validate it on their own. Given the vulnerability of communications, the increasing volume of available data, information, and intelligence, and the potential operational impact if the data, information, or intelligence is corrupt or misinterpreted, operational commanders are likely to demand continued intelligence participation, despite the expanded consumer access.

Another aspect of the ops-intel relationship potentially affected by the evolution of NCW is the procedure for maintaining the universal data stores on the information grid. Self-synchronization is predicated upon knowledge of the battlespace. Where the consumer is interacting directly with the data stores on the information grid to affect operations, they become the best source of the required updates to those stores, updates that were precipitated by their actions. That responsibility extends to the analysis and reporting of collateral affects, where an individual action produces multiple effects. In most if not all cases, data maintenance of this sort is beyond the manpower capabilities of the consumer.

The use of video from an unmanned aerial vehicle by an artillery battery to identify and subsequently strike an armored column serves as a case in point. The battery expended resources to identify the target and their actions changed the adversary's order of battle. The attack and the change in order of battle are required updates to the data stores to ensure the rest of the force has a current perspective of the battlespace. In this scenario, no one else in

the operation was charged to analyze the video or has direct knowledge of the action—the battery is the only immediate source for both. They can either update the data stores directly, or the commander can depend on a independent analysis to accomplish the updates. The former is more timely, the latter is less so, a duplication of effort, and may not rank high enough in the priority list of other activities to rate attention in time to make a difference. The best approach is to integrate the operations-intelligence team.

The evolution of NCW concepts must also consider the assignment of the activities that generate the data, information, or intelligence in the first place. Reducing the discussion to one of access alone ignores the myriad of steps often required to make data or information usable or useful. In some cases, it is not any single bit of information that has relevance, but a product that fuses many disparate and often unrelated bits of data or information into some usable form. Having access to the universe does not insure the right information will be found, or found within the time constraints imposed by operations, or have the proper classification.

The value of the COP, sometimes described as the omniscient view of the battlespace, must not be overstated. While extremely valuable, it is, in fact, a mere representation of the known and presentable facts at a given point in time. The sensor and information grids generate the discrete bits of data and information from the various disciplines, intelligence included, to create the prescribed or tailored view; viewers are left to draw their own conclusions.

The challenge in the evolution of NCW regarding the COP is to recognize the importance and complexity involved in the development of the underlying details and the fusion activities necessary to create it, and to avoid becoming fixated on the picture of the

moment. The more the data, information, or intelligence used to create the COP lends itself to an integrated display, and the closer the picture is focused on tactical operations, the better the COP supports decision making. However, at the operational level, the complexity of the problem, the breadth of potential operations, and security constraints increase the risk of the COP not containing all of the relevant data. Further, increased fusion of information, from a greater number of sources, and intuition are often central to effective decision making at the operational level. Neither fusion nor intuition is easily depicted on the COP. It must also be remembered that the picture is only refreshed as often as the communications and supporting infrastructure will allow. In sum, what the COP depicts may not be all the decision-maker needs to know; the commander must seek out the supporting analysis (i.e., the information or intelligence) to round out his or her view of the battlespace.

The U.S. Army's November 1997 Division AWE exemplifies some of the dangers associated with the COP. First, the exercise demonstrated that it is easy to become fixated on the real-time battlefield representations provided by a few systems, thereby reducing the importance and potential contribution of others assets providing input to the COP. This fixation can create a blind spot for the commander. Second, the dynamic retasking of collection assets may result in short term gains at the expense of overall performance, restrict the ability of the supporting assets to address overall needs of the operational force, and skew the operational view of the battlespace. Last, the COP does not diminish the importance of supporting analysis.⁶⁶ Others view the results quite differently. They conclude the commander of tomorrow will place greater emphasis on the accuracy of information rather

⁶⁶ William S. Wallace and William J. Tait, Jr., "Intelligence in the Division AWE: A Winner for the Next Millennium," Military Intelligence, vol. 24, no. 2, April-June 1998, 5.

than on analysis, that timing is everything.⁶⁷ Information is assumed to mean data or information in this context, while analysis is equated to information or intelligence. The challenge for the evolution of NCW (and for the planning and direction of intelligence) is to ensure the automated view of the battlespace, whether derived from a search of existing data stores or through the COP, represents the best aggregation of data, information, and intelligence possible.

While the preceding looked at the planning and directing of intelligence from a functionality perspective, another equally important consideration is the communications required to support it. Providing access to data stores to support decision making at the lowest possible level requires the expenditure of resources (dollars, communications assets, and personnel) to create and support the architecture.

Comparing communications capabilities in DESERT STORM and in Bosnia illustrate the advances in information technologies. In DESERT STORM, America's deployed forces received 1.3 million electronic messages in the first 30 hours.⁶⁸ In Bosnia, less than a decade later, what would have taken over an hour to transmit during the earlier operation can now be transmitted in seconds using commercially available technology.⁶⁹ Unfortunately, the operations in Bosnia also highlight several obstacles to extending the information grid. Systems like the Global Broadcast System (GBS) can move huge amounts of data forward, but have limited bi-directional capabilities. Interfacing satellite and tactical communications systems is difficult, and security of the data stores and the network is always an issue.⁷⁰ Further, commanders must carefully manage limited communications resources, allocating

⁶⁷ Garrett, 29.

⁶⁸ Kovacs, 402.

⁶⁹ Henry and Peartree, 127.

⁷⁰ Gompert, Kugler, and Libicki, 52.

connectivity and capacity to support their view of mission responsibilities and assigned tasking. Technology isn't the problem; policy and limited resources may deny parts of the operation the communications they deem necessary to support assigned tasking.

Security concerns underlie much of the preceding discussion, and have long been a source of misunderstanding between operations and intelligence. For intelligence, it is described as the green door behind which is thought to reside the answer to every question, but because of classification, is not shared with the operational force which lacks the proper clearance or need-to-know. Past successes, revised classification rules that provide greater access, and improved technology all serve to raise expectations within the operational community that intelligence has or should have the answer. With the increased complexity of the military problem set described above, that may not be the case. On the other hand, operationally generated need-to-know restrictions have sometimes limited intelligence participation in mission planning. Past 'intelligence failures', when combined with the green door perspective and operational restrictions imposed by sensitive operations distract from the required partnership essential to improving the intelligence support provided. Though both disciplines have worked hard to overcome these difficulties, security constraints will continue to complicate the evolution of the NCW concept.

In summary, discipline management should not fundamentally change with the evolution and promulgation of the NCW concepts and technologies. Successful military operations require a partnership in which all of the disciplines actively participate in the overall decision making process. The expanded access afforded by the information grid of NCW improves battlespace awareness throughout the force, increases the effective application of intelligence, and improves the dialogue (in substance and speed) between

operations and intelligence. Extending data access, in some cases, may require new data maintenance procedures, and will place increased demands on limited communications resources. While the intelligence process, including the associated planning and directing activities, is sound, the challenge for the commander is to remain fully engaged, as the fundamentals of NCW can potentially degrade operational efficiency and effectiveness.

Asset Management

Shifting focus from how NCW concepts may affect the assignment and execution of intelligence responsibilities, asset management evaluates how the intelligence planning and directing activities apply ISR assets and associated production, exploitation, and dissemination capabilities to an operational problem, and where they should be located. It is in this area that NCW perhaps offers the greatest opportunities for improvement. The following areas within the existing JID are those most affected.

The J-2 is charged with ensuring unity of effort for all intelligence assets supporting military operations, and for synthesizing the available data, information, and intelligence. As part of the planning process, the J-2 establishes intelligence needs (manpower, equipment, communications, logistic support, augmentees, and airlift) and priorities in the deployment plan, based on the commander's objectives and course of action.⁷¹

In most operations, only a subset of the organic or assigned intelligence assets will be forward deployed, requiring the JFC/J-2 to reach-back to obtain the essential support.⁷² Accordingly, the JFC must take steps to ensure access to all requisite theater and national intelligence capabilities.⁷³ The JCS and Combatant Command J-2 provide intelligence

⁷¹ Joint Chiefs of Staff, Joint Pub 2-0, II-4, III-1, IV-4 and 7.

⁷² Joint Chiefs of Staff, Joint Pub 2-02, I-1.

⁷³ Joint Chiefs of Staff, Joint Pub 2-0, IV-5.

support for the deploying force until its intelligence capability is established in the forward location. Throughout the operation, the Combatant Command's joint intelligence or analysis center (JIC/JAC) serves as the principal source of processing, exploitation, production, and dissemination support for the deployed force.⁷⁴ To augment the support package, the JFC can request a national intelligence support team (NIST) through the JCS/J-2, which deploys forward to coordinate the activities of all national agencies supporting the operation and the national command authority.⁷⁵

For coalition operations, there is no single intelligence doctrine.⁷⁶ Each presents a unique set of circumstances, a potentially new set of partners, and based on the commander's objectives and course of action, unique intelligence requirements. The J-2's responsibilities are the same; the operational environment is just more complex, and there are a larger number of participants in the decision-making process.

Critical to asset management is the continued primacy of the warfighting CINC. In military operations, and in the current JID, the CINC (or JFC) is the responsible party. Once intelligence assets are allocated to the operation, they must become subordinate to the commander. Centralized planning and direction, and decentralized execution must not fall victim to the potential of the automation and increased insights, perspectives, and participation afforded by the concepts of NCW.

Per the JID, unity of effort for intelligence draws its focus from the commander, and is the objective of the planning and directing activities. In some ways, it crosses the artificial boundary between asset and task management established in this analysis. In the details,

⁷⁴ Joint Chiefs of Staff, Joint Pub 2-0, VII-7, and Joint Chiefs of Staff, Joint Pub 2-01, III-27-29.

⁷⁵ Joint Chiefs of Staff, Joint Pub 2-02, V-5.

⁷⁶ Joint Chiefs of Staff, Joint Pub 2-0, VIII-1.

unity of effort has much in common with self-synchronization. The goals of both are increased combat effectiveness and efficiency. Once fully deployed the information grid becomes a common enabler. The key aspect of unity of effort is to ensure everyone is working towards the same objective with the least amount of redundancy and overlap on a timeline that supports the ongoing operation.⁷⁷

From an intelligence asset management perspective, unity of effort can be improved by providing increased visibility for the commander's intent, the information needs and shortfalls of the deployed force, and the daily requests for support generated by ongoing operations. With the information grid as the enabler, intelligence assets (organic, attached, or supporting) can actively participate in deciding what needs to be done and how best to meet the needs of the deployed force, that is, to self-synchronize their efforts and avoid redundancy. The visibility afforded by the grid also allows management to balance task assignments to effectively employ unused capacity, or to react to production delays or information shortfalls before either can affect ongoing or planned operations. In essence, it moves the entire force from reacting to acting, a critical shift in supporting increased speed of command.

Clearly this is the ideal; several hurdles must be overcome before the ideal can become the reality. As the earlier JCS/J-6 citation indicated, the requisite C⁴ infrastructure isn't fully fielded, and the funding to do so is not a given. Combined operations simply increase security and interoperability challenges. Unity of effort also requires adaptive organizational relationships and the dynamic reassignment of assets to meet mission needs.⁷⁸

⁷⁷ Ibid., IV-4.

⁷⁸ Ronald D. Elliott, "Agile Intelligence Enterprise Offers Requisite Flexibility," SIGNAL, vol. 53, no. 2, October 1998, 81.

These latter two mandate a rethinking of resource allocation and tasking authority, issues that involve both management prerogatives and funding constraints.

Every asset in the DOD is subordinated somewhere in the hierarchical organizational structure of the department. As such, the responsible party controls the tasking, priorities, and expenditure of resources for their subordinate activities. For intelligence, funding is provided from various defense accounts dependent on the focus of the organization and the community it supports. These are two major constraints that must be overcome.

All of the intelligence agencies within the IC would report they are gainfully and fully employed. Major intelligence organizations (i.e., Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, and the combatant command JIC/JACs) have continuing production responsibilities as part of the DOD Intelligence Production Program (DODIPP). Dynamic requests for support or information are generated through the RFI and CM process.

In peacetime, there is no incentive to willingly provide additional capacity to interests or tasks outside the agency's area of responsibility. In fact, just the opposite is true from a programmatic perspective. Annual budgets are justified on a specific mission statement and organizational charter that establish production responsibilities and limitations. Voluntarily committing resources beyond legislated authority draws oversight attention. Committing to additional tasking without direction or authorization exhibits excess capacity, and raises questions about the validity of existing tasking or manning. Either way, the organization is not rewarded. Thus, while having insight into the needs of the community will enhance the delivered product, it will not increase the tasking an organization accepts, nor the amount of

resources they are willing to expend outside their normal purview, nor the priority of those they routinely accept. This must change.

Funding is a legal issue that involves congressional oversight. Paying for extensions to the information grid (or any other aspect of NCW for that matter) is constrained by the funding source. While a particular extension of the information grid may be in the interest of the DOD, funding from the proper source must be available.⁷⁹ This is especially difficult where systems or extensions funded from different sources interface. In crisis and war, funding limitations are often transparent (or simply ignored). The Services simply expend the necessary funds required to accomplish the assigned tasks. Given American high-tech, high-speed operations, that often involves the fielding of additional capabilities central to the NCW concept. In most cases, supplemental appropriations are provided by Congress to cover the cost of the operation; where this is not the case, funds are transferred from existing Service accounts, often at the expense of training, readiness, or procurement. In MOOTW or for peacetime activities, expending resources from one fund on activities outside the purview of that fund is difficult, hence the promulgation of NCW technologies is much more complicated. Whether accomplished during peace or war, once fielded, these capabilities must be maintained, and are therefore a continual drain on limited DOD resources. To facilitate both the fielding and long-term maintenance of NCW technologies, procedures for moving money and an ability to reach across programs for the common good are much needed improvements.

The concepts of NCW also have the potential for greatly enhancing the J-2's ability to synthesize intelligence. Physically extending the information grid, standardizing data

⁷⁹ Lt Col Marianne Carter, JCS/J-6T, C4 Systems, Networks Division, interview by authors, 30 March 1999, Pentagon, Washington, D.C., interview notes.

labeling, expanding access to data stores containing data, information and intelligence, improving storage and retrieval algorithms, and integrating specialized data processors into the grid are essential improvements currently being pursued. Collectively, these improvements increase timeliness, enhance opportunities for data verification and validation, and the ability to correlate and fuse data, information, and intelligence into products tailored to operational needs. They also enable the IC to anticipate shortfalls and security constraints, and to expand the kinds of data, information, or intelligence available for synthesis.

Continued migration towards the architecture outlined above, which also includes multimedia and multi-level secure operating systems, along with advanced collaborative analytical tools,⁸⁰ allows the DOD to reconsider the need to forward deploy resources as a central theme in asset management. In the past, the operational force had to physically deploy the functional support it required; the foundations of networks in NCW provide the alternative of reaching back through the network for the required support. If fully embraced and supported by required communications and necessary changes in resource allocation and tasking authority, reach back could significantly change the way the functional aggregation at the JIC/JACs, and eliminate the need for the NIST in the forward area.

At the organizational level, the U.S. Air Force's Contingency Airborne Reconnaissance System (CARS), the ground processing and exploitation system for the U-2, already supports forward deployed forces from its bases in the continental U.S.. Mission materials are sent from the collector operating in the forward area (NCW's notional sensor grid) to the ground station for processing and exploitation (all part of NCW's information grid). Resultant data, information, and intelligence is transmitted to users around the world

⁸⁰ Elliot, 79.

for local storage and consumption (again, part of NCW's information grid) in time to effect ongoing operations.

At the functional level, the U.S. Air Force's 1998 Expeditionary Force Exercise (EFX98) demonstrated the capability to divide the air operations center, sending parts of it forward while the rest remained in garrison. Through the exercise, the center remained fully functional and capable of providing requisite support during the force deployment phase (another mission enhancement the information grid affords) as well as during extended operations.

For the JIC/JACs, does the evolution towards the concepts of NCW portend a day when the organization will become virtual, drawing its required assets and support across the network, rather than physically co-locating them in the forward operating area? The information grid is already providing access to additional data stores and a flow of information that continually updates situational awareness. Both greatly enhance the organization's ability to satisfy unit tasking and to anticipate problems throughout their area of responsibility. The foundations of NCW provide a 'virtual' option for the future evolution of these organizations.

In reality, virtual intelligence organizations face significant obstacles. The existing C⁴ infrastructure isn't capable of providing the requisite connectivity, throughput, or capability. Questions of vulnerability and reliability must also be resolved. Resource allocation and task management procedures, along with funding restrictions must all be modified to allow inter-organizational problem solving. Perhaps as critical as anything, remotized assets must evolve to become the norm vice the exception. Today, a commander takes comfort in the physical presence of assigned organizations and functions.

The same doesn't necessarily apply to the NIST. This entity is already a forward-deployed representative of a much larger intelligence apparatus. The NIST provides this apparatus a valuable forward presence, a hands-on view of the operation to which it is committing resources, and a means of synchronizing and deconflicting the activities of all of the participants. As such, the team helps clarify support requirements and enables the agencies it represents to anticipate additional workload or intelligence needs. To the forward force, the team is a valuable resource that can assume management of tasks or functions that would ultimately consume organic resources. However, the team requires the same support as any other deploying asset. In addition, while teams often bring communications capabilities, the force they are supporting must provide the connectivity.

What the NCW concept suggests is not deploying the NIST. Fundamentally, it already works through an information grid to energize the supporting agencies. It operates under JCS/J-2 control, so co-locating the two also has administrative advantages. To the deployed force, reducing the number of people forward reduces support requirements, which must never be overlooked. The obvious downside is the same dependence on communications, and the loss of direct face-to-face contact with the commander and the deployed forces cited above.

In summary, the fundamentals of NCW offer several opportunities to improve asset management. Unity of effort and intelligence synchronization are enhanced by the connectivity of the information grid and the insights it provides. This insight also allows both the operational commander and the supporting activities to anticipate requirements and take actions to improve responsiveness and thereby improve speed of command. In the near term, the fundamentals of NCW allow the operational force an option of foregoing the

forward deployment of the NIST. In the future, the same principles and capabilities that allow the command to forego the forward deployment of the NIST could be applied to reducing the size of the JTF/J-2 staff elements, and in the longer term, creating a virtual JIC/JAC. These opportunities do not stretch the realm of possibility, but must certainly be considered in the reality of today. Communications limitations and resource constraints must be overcome, and management practices must evolve if these opportunities are to be pursued.

Task Management

In the final area of the analysis, Task Management, the research focused on NCW's potential impact on the intelligence planning and direction activities that: generate the information used in operational planning; provide responses to requests for support or for data, information, or intelligence; or provide support to those tasks assigned to intelligence during the conduct of military operations. The literature on NCW to date is silent on the details of task management, but the underlying principles offer opportunities to improve the current process.

Within the JID, the intelligence community plays a key role in planning for and executing military operations. At the operational level, the J-2 is the principal for developing the commander's estimate of the situation, and makes significant contributions towards the development of operational objectives and alternative COAs. Intelligence also develops the target list once the COA is determined, and conducts the combat and bomb damage assessment (CA/BDA) once operations get underway. Throughout, intelligence is charged with maintaining situational awareness; for keeping the decision makers apprised of the adversary's will, capabilities, intent, objectives, and alternatives; and for responding to requests for support.

Dependent on the request, planning and direction activities in task management are executed through the RFI, CM, or PR processes. The Combatant Command J-2 is charged with eliminating duplication of effort and avoiding redundancy.⁸¹ It is also responsible for ensuring that requests for intelligence are satisfied at the lowest possible level. Where national systems collection is required, the Joint Staff J-2 and DIA assure it is integrated with the all-source analytical strategy.⁸²

One of the potential improvements the NCW construct offers is the fidelity with which assets can be tasked. Currently, tasking (requests for information, support, or collection) and the resultant processing, exploitation, or dissemination activities are managed at the organizational level, regardless of the type of request or who responds. Collaboration initiatives (i.e., the Joint Intelligence Virtual Architecture) are intended to reach below the organizational level to the individual assets. Collectively, providing asset visibility and a means to employ them below the unit level can increase overall efficiency and responsiveness to operational needs as capabilities can anticipate and engage, rather than wait and react, or be restricted by organizational boundaries. Collaboration across the information grid not only improves the delivered product but also eliminates the need to or the expense of physically relocating them. This obviously assumes necessary communications connectivity, security authorization, procedural changes in resource allocation and tasking authority, and relief from funding constraints.

Like much of the operational world today, requirements management systems are stovepiped, supporting a very specific community through direct connectivity. In and of themselves, they follow the fundamentals of NCW's information grid, but visibility is limited

⁸¹ Joint Chiefs of Staff, Joint Pub 2-01, II-9, III-7 to 25 and 38-40.

⁸² Joint Chiefs of Staff, Joint Pub 2-0, VI-3 and 9.

to the community they support due to system architecture or security constraints. Many of these systems are also discipline specific, and some are limited to supporting just portions of the community or portions of the intelligence cycle (Figure 3). Efforts like the Integrated Collection Management (ICM), advanced concept technology demonstration (ACTD), and the Joint Collection Management Tool (JCMT) are attempts to integrate RFI and collection management, and to provide more powerful software support tools to improve intelligence collection and production strategies. What is missing is visibility into the entire requirement process and a warfighting perspective in the management philosophy.

In order to realize the potential of the constructs articulated for NCW, intelligence needs to rethink the management of requirements. First, the definition of requirement must be expanded to include requests that generate action anywhere in the intelligence cycle, and all requirements must be managed as an aggregate. While the current doctrine articulates in great detail how to plan and direct collection and related processing and production activities, it spends little time on RFI management, and less on production requirements that affect the DODIIP. Local TTPs implement the process, much of which is manual. Further, programs like Information Dissemination Management (IDM) introduce a new form of requirement. IDM, based on guidelines approved by the commander, establishes automatically dissemination activities. The dissemination itself, the subsequent storage and maintenance of the deliverable, and the tasks that the deliverable supports all consume operational resources. To achieve the efficiencies afforded by advances in information technology and the effective use of limited intelligence resources, the requirement process must be all-inclusive.

Lastly, the integrated requirement process outlined above must track a request through the entire cycle: from generation, through the expenditures of resources in whatever

combination or form, to product dissemination. It must also include a means for automated feedback. Today, portions of the cycle are excluded. For example, collection operations management activities (a part of CM) are not fully integrated into the requirement process. Further, the current requirement process does not tie the delivered product to the original request, particularly when the deliverable is an aggregation of various source materials. The process must also provide a means for tracking resource commitments and expenditures. This is particularly important when assets from one or more organizations collaborate to generate the final product. While the fundamentals associated with NCW provide opportunities, the basic requirement process must first be revised. Reflecting on the concerns of Secretary Money cited earlier in the paper, to do otherwise will simply automate a poor process.

CONCLUSIONS

The networking of intelligence collection, production, and dissemination assets, and their associated data stores, consistent with the fundamentals of NCW, provide tremendous opportunities for improving intelligence support to operations. Fundamentally, the existing JID is sound, though as one might expect, it was written to reflect a former time that did not have many of the capabilities inherent in the NCW construct. The increased access and visibility NCW concepts afford do not decrease the need for intelligence, but will undoubtedly improve the management of the discipline itself and the dialogue between intelligence and its customers.

With better questions, and a means for anticipating the needs of the operational force, the IC can be better postured to provide timely and tailored products to the operational force. Real- or near-real-time requirements, like the COP and sensor-to-shooter applications, are

enabled by the NCW grids, which facilitate improvements in the supporting intelligence activities and provide the essential connectivity to deliver products to the consumer in a timely manner. Improvements in data management applications and networking technologies greatly increase the capability to correlate and fuse data, information and intelligence, which not only facilitates the teamwork outlined in the current intelligence doctrine, but the effectiveness of the support provided by the discipline.

The increased connectivity central to NCW, and the visibility it provides, can also facilitate the self-synchronization of the IC, which leads to greater unity of effort, in its support to military operations. Having insight into anticipated information needs and shortfalls within the context of the operational commander's intent allows the IC to engage in decision making rather than react to tasking after the fact. This approach contributes to increased speed of command and support to real-time requirements like the COP and sensor-to-shooter applications.

Networking can also lead to a revision of the need to forward deploy intelligence assets and capabilities. Initially, the need for the NIST to go forward is functionally eliminated. In the longer term, as the fundamentals of NCW are fully promulgated, virtual organizations tasked at the internal capability vice organizational level, which collaborate in problem solving, are possible. By reducing the need to deploy the entire support structure, these opportunities reduce military reaction times and the number of assets put directly in harm's way, while increasing the amount intellectual power and technical capability applied to a military problem.

Applying the principles of NCW to task management enables a rethinking of the entire requirements management process. First, the community must overcome the stove

piping inherent in the current requirements management systems and view requirements in the aggregate. Such a shift would be consistent with the fundamental philosophy of NCW, and would provide many of the same advantages. In the tasking process itself, the technology and management philosophy associated with NCW also provides several opportunities for improvement. It supports the tasking of intelligence assets below the organizational level, critical to the efficient use of collaborative production efforts. It facilitates the management of the improved dissemination capabilities introduced by IDM. Further, it allows the tracking of tasks from initial generation to product delivery. Collectively, it is the intelligence discipline that must integrate the NCW concepts and underlying philosophy to effect improvements in the tasking process.

One should overlook neither the complexity nor the amount of work remaining before these advantages are realized. Technically, the fundamentals of NCW are quite straightforward. What is required is a management commitment to funding and fielding the requisite infrastructure; a decision that must be made in the context of all of the competing interests in a resource constrained environment. Perhaps more important are significant changes in management philosophy that must precede or at a minimum accompany the promulgation of the capabilities. The operational force must guard against accepting the data, information, or intelligence on the net at face value, or downplay the need for supporting analysis. Management must also revise the fundamentals of resource allocation and tasking authority to take full advantage of the evolving technical opportunities. Restriction in the execution of funds must also be overcome. Lastly, security must always be considered in network design and functional allocation of tasking, particularly in coalition operations.

In summary, the existing JID must continue to evolve to take advantage of the advances in information management and networking technologies, the cornerstones of NCW. The fundamentals outlined in current publications continue to be relevant, but must be updated to place less emphasis on physical location and more on the revised management concepts and functional relationships evolving out the continuing promulgation of technology throughout the operational forces.

RESEARCH CONCLUSIONS

This research found that the doctrine and TTPs that guide the planning and direction of intelligence at the operational level appropriately incorporate some of the technology and underlying principles associated with NCW. They rightly lag behind the evolution of the NCW concept, as doctrine reflects the foundation for military operations based on principles derived over time. Doctrine is not meant to rapidly change to capture the latest fad, but to evolve more slowly to allow potential revolutionary changes to mature. TTPs must necessarily describe how existing or known capabilities will be applied to potential military problems. That is not to say the doctrine and TTPs do not incorporate NCW principles or technology, but rather like the concept itself, they reflect an ongoing evolution.

The concepts associated with NCW offer significant opportunities for dealing with the challenges facing intelligence and the military in general in the 21st century. Information dominance, built on advanced networking and information management technologies, is the key enabler for meeting the objectives outlined in JV 2010, the DOD's vision for meeting those challenges. The connectivity of NCW's grids (information, sensor, and shooter) coupled with improved command and control, simply put information dominance in an

operational perspective. Increased speed of command, getting data into the hands of the operational force in the proper format and in time to make a difference, is the intended result.

Improved data management, combined with increased communications connectivity and capacity, serves to enhance the utility and usefulness of the grids. The additional insight flowing from the grids not only improves battlespace awareness, but highlights information shortfalls and improves communication between intelligence and its customers, and thereby the support intelligence provides (a derivative of enhanced planning and direction activities). With increased networking also comes a corresponding potential to reduce deployment requirements, while simultaneously increasing access to special analytic or production resources. The grids also offer an opportunity to improve resource management, looking at requirements for data, information, and intelligence in the aggregate with less emphasis on discipline or organizational boundaries. Collectively, these capabilities provide an opportunity for the operational force and, more specifically, for intelligence to anticipate requirements and to self-synchronize their activities (the other key tenet of NCW), thus improving the effectiveness and efficiency of military operations.

Both the doctrine and the TTPs incorporate many of the advances in networking and data management technologies inherent in the NCW concept. Employing commercially driven technologies, more military assets are being networked, and the networks are being extended to a broader base of consumers. Network capacity available to the operational force is being increased with the fielding of new satellite-based infrastructure, the GBS being a prime example. Combined with policy changes, access restrictions (physical connectivity or security constraints) are being removed, providing expanded access to formerly restricted data, information, and intelligence stores. These changes support the direct application of the

material (i.e., the COP and sensor-to-shooter applications), which reduces the time consumed by the 'observe and orient' portions of the decision cycle and thereby improves speed of command. The expanded access also ensures better-informed decision making, and an opportunity to anticipate operational needs.

Advanced employment concepts involving remoted application of resources, another opportunity of the NCW construct, are being demonstrated throughout the DOD. The Air Force's CARS ground stations currently provide direct support to operational forces around the world without leaving home base. The Army's DAWE is another case in point. With JIVA, the department is pursuing new applications for virtual collaboration across the network, which when fully developed, will provide additional opportunities to reduce deployment requirements while increasing direct intelligence support to operations. In resource management, integrated applications like JCMT and ICM are being developed to improve the effectiveness and efficiency of the tasking process. While not referred to as NCW initiatives, these examples are based on extensions of the same principles.

What the doctrine and TTPs do illustrate, however, is that while an evolution is underway, there are several significant challenges which must be overcome. The importance of the commander and the need to make operational decisions in the forward area is not changed with technology; it is merely enhanced. The skepticism with which intelligence and operations view one another is not eliminated by improvements in technology, but technology can improve the basis for dialogue and the insights required to minimize it. In the actual execution of responsibilities, self-synchronization does not reduce management or supervisory responsibilities, but may make them more complex.

Though there are many examples of networked capabilities, the doctrine and the TTPs both reflect a traditional hierarchical management philosophy, and a tendency to co-locate assets in the forward area when possible. Organizational boundaries will remain a challenge to potential enhancements in resource allocation and tasking authority made possible by networking and advances in data management. Funding constraints will also prolong the evolution, for the sources are established by legislation and therefore can't be modified through changes in procedures. Likewise, security constraints will continue to complicate the evolution, particularly when sensitive sources and methods are used and when military operations involve coalitions.

Lastly, while technology is not a problem, extending the network to keep pace with the evolution and to provide all of its potential, presents a combination of challenges. For management, determining who needs what access for what purpose is critical, as the decision determines communications connectivity, capacity and access requirements. It also establishes requirements for manpower to implement and maintain the capability and the associated data stores, and the funding necessary to buy or lease capacity, procure the equipment, and sustain the people. This decision also defines the security environment, which may levy additional resource requirements. Funding for all of this must be properly programmed and appropriated, which further complicates the operational decision.

To avoid security issues, more detailed comments about the TTPs and the evaluation of the NCW concept in a real-world operation are deferred to the respective annexes themselves. Suffice it to say, like the doctrine, both the TTPs and in its practical application, the evolution of the NCW concept is underway.

In summary, the DOD is actively pursuing the operational objectives of JV 2010. The NCW concept is but another way of exemplifying the fundamentals required to achieve information dominance, its key enabler. In the details, the DOD is evolving both in technical and managerial terms, incorporating into the intelligence doctrine and TTPs as appropriate, those aspects of the NCW construct mature enough to improve the effectiveness and efficiency of combat operations. Within managerial, operational, funding and security constraints, an evolution is underway; the concepts of NCW, or more broadly, those of information dominance, lie at the heart of that evolution.

RECOMMENDATIONS

The concepts and enabling technologies of NCW offer many opportunities for improving the planning and direction of intelligence and the resultant support to operations; however, there are many challenges which must be overcome as well. The following five recommendations, representing some of the most significant issues highlighted by the research itself, are offered to enhance the continued evolution of the NCW concept.

The acquisition of technology and the promulgation of NCW concepts by the DOD, and more specifically intelligence, must be paced to allow the technology to mature and the management concepts to evolve so that this does not become simply a technology insertion. To take full advantage of the concept requires that it be fully integrated into the intelligence doctrine and TTPs. To do otherwise ensures that NCW will merely mature as a faster way of doing what we do today, automating many of the currently stove-piped, platform-centric processes, and ignoring much of the potential the concept offers.

Changes in management philosophy must coincide with the elimination of stovepipes and 'lanes in the road'. The current environment depends upon organizational expertise and

boundaries. NCW offers an opportunity to integrate individual skills and a greater variety of expertise from geographically separated organizations throughout the IC, and to allow them to collaborate across the network to improve the quality, content, and timeliness, and hence the relevance, of the support provided. To take advantage of these opportunities requires adequate communications, changes in the tasking process and the management of resources (to include funding), and a way to overcome security constraints. Actions that address these issues require management direction and support.

Changes in the way the IC is funded must be made from a corporate standpoint with congressional involvement. Incentives must be provided for an organization to acknowledge an intelligence shortfall and attempt to fill it even though the requestor may not be on their current list of supported agencies, a key concept of self-synchronization.

A comprehensive education and training process must evolve coincident with the NCW concept. As the networking construct is promulgated, consumers (and senior leaders in particular) must be conditioned to ask for data, information, and intelligence, not platforms. RFIs must serve as the basis for requesting support; the importance of where the response is generated or by whom should be reduced. The key is getting management on board. The IC itself must devise TTPs that take full advantage of the evolving potential, and must update the training and skills levels as the capabilities are fielded.

Security issues must be resolved as the movement toward the NCW environment continues. With many, if not all, future military operations involving a coalition of some sort, current foreign disclosure policies and classification guidelines are inadequate. A methodology that facilitates the effective use of U.S. intelligence while simultaneously protecting sensitive sources and methods is essential.

To help shape the argument or concern, and to facilitate the continued evolution of not only the NCW concept but its application to the planning and direction of intelligence as well, additional analysis is recommended in the following areas.

- ✓ Management philosophy. Should the IC manage assets at the sub-organizational level in a network-centric environment, and if so, how? What functions should be performed where and by whom?
- ✓ Task Management. Identify the alternatives for task management in a network-centric environment. What impact will self-synchronization have on the alternatives and the resultant TTPs?
- ✓ Characterization of the battlespace. How does NCW affect the physical characterization of the battlespace and the linear conduct of war? Are the concepts of parallel targeting, branches and sequels, and self-synchronization compatible in an NCW environment?
- ✓ Data architecture. From an operational perspective, how is data, information, or intelligence verified and validated in a network-centric environment? Where should the data stores be located, and who should be responsible for maintenance of the individual data and the database itself? What connectivity and accessibility is required?
- ✓ Communications. Beginning from management perspective above, what connectivity, capacity, and access is required to support it?
- ✓ Security. Detail the impacts security has on the continued evolution of network-centric concepts. Does the DOD need a multi-level secure operating environment, and what are its advantages/disadvantages?

- ✓ Training. What training is required to keep pace with the concepts and technologies associated with NCW, and what changes must be made in the current process?
- ✓ Funding. Does NCW really necessitate a change in the way the IC funds its activities today? If so, how and when should that change occur?

Together, these issues represent the principle challenges the DOD must address as it continues develop the concepts associated with NCW and field the enabling technology.

BIBLIOGRAPHY

- Adams, Thomas K. "Radical Destabilizing Effects of New Technologies." Parameters, U.S. Army War College Quarterly, vol. XXVIII, no. 3, Autumn 1998, 99-111.
- Ackerman, Robert K. "Air Force Communications Experts practice Expeditionary Operations." SIGNAL, vol. 53, no. 3, November 1998, 21-24.
- _____. "Air Intelligence Confronts New Geopolitical Realities." SIGNAL, vol. 53, no. 2, October 1998, 227-29.
- _____. "Information Age Poses New Challenges to Intelligence." SIGNAL, vol. 53, no. 2, October 1998, 23-25.
- _____. "Information Technologies No Longer Limit Command Center Developments." SIGNAL, vol. 53, no. 3, November 1998, 63-65.
- _____. "Pacific Communications Span Broad Gulf of Hemisphere." SIGNAL, vol. 53, no. 2, October 1998, 40-42.
- Ball, Randy. "Joint Collection Management Tools." Briefing Slides. Presented as part of the Advanced Cooperative Collection Management (ACCM) Program Briefing. Washington, D.C.: 15 July 1997.
- Barnett, Thomas P. M. "The Seven deadly sins of Network-Centric Warfare." U.S. Naval Institute Proceedings, vol. 125/1/1, 151, January 1999, 36-39.
- BDM International and Science Applications International Corporation. JCS/J6 Warfighter Communications Study. Washington, D.C.: 23 February 1998.
<<http://199.114.114.220/wfcomm/index.html>> (7 December 1998).
- Barnett, Roger W. Memorandum for Record, 11 January 1999. "A Critical Review of 'The Seven Deadly Sins of Network-Centric Warfare' by Thomas P.M. Barnett, U.S. Naval Institute Proceedings, January 1999." Naval War College, Newport, RI.
- Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." SIGNAL Information Warfare Series, n.d., pp. 23-24, 27.
- Brewin, Bob. "DOD lays groundwork for network-centric warfare." FCW Editorial Supplement, 10 November 1997.
<http://www.idg.net/new_docids/departments/defense/g>
<http://idg.net/idg_frames/english/content.cgi?vc=do> (12 Feb 99)

- Britten, Scott M. "Reachback Operations for air Campaign Planning and Execution." Occasional Paper No. 1, Center for Strategy and Technology, Air War College, Maxwell AFB, AL: September 1997.
- Brohm, Gerard P. "C4IEWS: The Enabler of Information Dominance." Military Technology, no. 5, May 1998, 7-11.
- "Budgets." Air Force Magazine, vol. 82, no. 5, May 1999, 56-61.
- Callum, Robert. "Will Our Forces Match the Threat?" U.S. Naval Institute Proceedings, vol. 124/8/1,146, August 1998, 50-53.
- Campen, Alan D. "Assessments Necessary in Coming to Terms with Information War." SIGNAL Information Warfare Series, n.d., 28-29.
- Carter, Marianne. JCS/J6T, C⁴ Systems, Networks Division. Interview by authors. 30 March 1999. Pentagon, Washington, D.C.. Interview notes.
- Cebrowski, VADM Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." U.S. Naval Institute Proceedings, vol. 124/1/139, January 1998, 28-35.
- Cebrowski, VADM Arthur K. "Network-Centric Warfare." Briefing Slides dated 23 Apr 98. <<http://spica.or.nps.navy.mil/netusw/cebrowskinetwar/sld 001-016.html>> (12 Feb 99)
- Central Intelligence Agency. Intelligence Systems Board. Intelligence Community Information Systems Strategic Plan FY 1999-2003. Washington, D.C., November 1997.
- Commission on the Roles and Capabilities of the United States Intelligence Community. Preparing for the 21st Century, An Appraisal of U.S. Intelligence. Washington, D.C., 1 March 1996.
- Cradock, Percy. Book Review: Intelligence power in peace and war, written by Michael Herman. Cambridge: Cambridge University Press, 1996. Published in International Affairs, vol. 73, no. 4, October 1997, 785-787.
- Defense Advanced Research Projects Agency (DARPA/ISO). "Command Post of the Future." Briefing Slides, presented by David Gunning and Marshall Reed., n.d..
- Defense Intelligence Agency. JIVA Integration Management Office. Concept of Operations for Community of Interest (COI). Washington, D.C., 29 September 1998. <<http://www.dia.smil.mil/proj/jiva/docs/COIconops.html>> (11 January 1999)
- _____. JIMO Points of Contact. Washington, D.C., 27 July 1998. <<http://www.dia.smil.mil/proj/jiva/poc/jimopoc.html>> (11 January 1999)

_____. Joint Intelligence Virtual Architecture Briefing. Washington, D.C., n.d..
<http://www.dia.smil.mil/proj/jiva/brief/JIVA_BRIEF/sldXXX.html> (11 January 1999)

_____. Joint Intelligence Virtual Architecture (JIVA) Collaborative Environment (JCE) Draft master Implementation Plan (JMIP). Washington, D.C., 30 October 1998.
<<http://www.dia.smil.mil/proj/jiva/docs/JMIP/MIP.html>> (11 January 1999)

Dahl, Erik J. "We Don't Need an IW Commander." U.S. Naval Institute Proceedings, vol. 125/1/1, 151, January 1999, 48-49.

Dunlap, Charles J. "Joint Vision 2010: A Red Team Assessment." Joint Force Quarterly, no. 17, Autumn-Winter 1997-1998, 47-49.

Dunmire, Brian R. "Collection Management Lessons Learned During the Division AWE." Military Intelligence, vol. 24, no. 2, April-June 1998, 16-20.

Echevarria, Antulio J., II. "Tomorrow's Army: The Challenge of Nonlinear Change." Parameters, U.S. Army War College Quarterly, vol. XXVIII, no. 3, Autumn 1998, 85-98.

"EFX '98 Preliminary Results." Air Force Policy Letter Digest, December 1998.
<<http://www.af.mil/lib/policy/letters/pl98-12.html>> (January 21, 1999).

Elliott, Ronald D. "Agile Intelligence Enterprise Offers Requisite Flexibility." SIGNAL, vol. 53, no. 2, October 1998, 79-81.

Eriksson, Par. "Intelligence in Peacekeeping Operations." International Journal of Intelligence and Counterintelligence, vol. 10, no. 1, Spring 1997, 1-18.

"Expeditionary Aerospace Power." Air Force Magazine, vol. 81, no. 11, November 1998, 4-6.

Frame, John E. "Intelligence Planning in the Digital Division." Military Intelligence, vol. 24, no. 2, April-June 1998, 13-15.

Galik, Dan. "Defense in Depth: Security for Network-Centric Warfare."
<http://www.chips.navy.mil/chips/archives/98_apr/Galik.html. (12 Feb 99)

Garrett, Stephen F. "Evolving Information-Age Battle Staffs." Military Review, vol. LXXVIII, no. 2, March-April 1998, pp. 28-31, 35-36.

Gompert, David C., Richard L. Kugler, and Martin C. Libicki. Mind the Gap, Promoting a Transatlantic Revolution in Military Affairs. Washington: National Defense University Press, 1999.

- Gray, Colin S. "RMAs and the Dimensions of Strategy." Joint Force Quarterly, no. 17, Autumn-Winter 1997-1998. 50-54.
- Hart, Marsha. "Integrated Collection Management Advanced Concept Technology Demonstration (ICM ACTD)." Briefing Slides. Presented as part of the Advanced Cooperative Collection Management (ACCM) Program Briefing. Washington, D.C.: 15 July 1997.
- Henry, Ryan, and C. Edward Peartree. "Military Theory and Information Warfare." Parameters, U.S. Army War College Quarterly, vol. XXVIII, no. 3, Autumn 1998, 112-135.
- Holland, Rear Admiral W. J. "Nuclear Weapons in the Info Age: Who Needs 'em?" U.S. Naval Institute Proceedings, vol. 125/1/1,151, January 1999, 45-47.
- Huber, Arthur F., Philip S. Sauer, J. Lawrence Hollett, Kenneth Keskel, William L. Shelton, Jr., and John T. Dillaplain. The Virtual Combat Air Staff, The Promise of Information Technologies. Santa Monica, CA: RAND, 1996.
- "Information and Command & Control." Aerospace America, December 1997, 42-42.
- Jenkins, James T. "Use Technology . . . Don't Trust It!" U.S. Naval Institute Proceedings, vol. 124/8/1,146, August 1998, 69-70.
- Joint Warfighting Center. Joint Task Force Commander's Handbook for Peace Operations. Fort Monroe, VA: 1995.
- Kagan, Mark H. "Global Satellite Datalinks Connect Fixed, Mobile Users." SIGNAL, vol. 53, no. 4, December 1998, 21-24.
- Kovacs, Amos. "The Nonuse of Intelligence." International Journal of Intelligence and Counterintelligence, vol. 10, no. 4, Winter 1997-1998, 383-417.
- LaChance, Michael A. "The Digital Planning Process: Lessons Learned from the AWEs." Military Intelligence, vol. 24, no. 2, April-June 1998, 9-12.
- Lee, Deborah R. "Proving the Value of an Integrated Total Force." The Officer, vol. LXXIV, no. 13, April 1998, 31-34.
- Loescher, Michael S. "Moving the Navy Into the Information Age." U.S. Naval Institute Proceedings, vol. 125/1/1,151, January 1999, 40-44.
- "Major Reorganization of DoD's C3I Office Impacts DARO, Information and Space Systems." Journal of Electronic Defense, vol. 21, no. 6, June 1998, 16.

Money, Arthur L. U.S. DoD Chief Information Officer. Interview by Bryan Bender, published in Janes Defense Weekly, vol. 30, no. 10, 9 September 1998, 96.

National Imagery and Mapping Agency. Imagery and Geospatial Community Operations Vision into the 21st Century (Draft, Version 1.0). Washington, D.C.: 31 March 1998. <<http://www.nima.smil.mil/information/organization/igc-vision/dd-msg.html>> (26 January 1999).

_____. IGC Operations Vision into the 21st Century, Draft Terms of Reference (TOR). Washington, D. C.: 2 April 1998. <<http://www.nima.smil.mil/information/organization/igc-vision/tped/tor.html>> (26 January 1999).

Pace, Howard, Jr., and Phillip E. Pace. "Frequency Management for the 21st Century." Journal of Electronic Defense, vol. 21, no. 1, January 1998, 45-48.

Peters, F. Whitten, U.S. Air Force Acting Secretary, and Gen Michael Ryan, Air Force Chief of Staff. Air Expeditionary Forces. DoD Press Briefing on August 4, 1998, txt pp. 1-19, and slides 1-19. <<http://www.af.mil/lib/misc/eafbrief.html>> (22 January 1999).

Peters, F. Whitten. U.S. Air Force Acting Secretary. Interview by Greg Seigle, published in Janes Defense Weekly, vol. 30, no. 22, 2 December 1998, 40.

Podlesny, Robert E. "Infrastructure Networks Are Key Vulnerabilities." U.S. Naval Institute Proceedings, vol. 125/2/1,152, February 1999, 51-53.

Richard, Dana G. Global Broadcast Service Primer. n.d.. <<http://www.j2aic.acom.smil.mil/gbs/gbsprimer.html>> (19 January 1999).

Robinson, Clarence A. "Allied Command Europe Harnesses Digital Communications Advances." SIGNAL, vol. 53, no. 1, September 1998, 17-20.

_____. "Commanders Gain Global Access Through Commercial Equipment." SIGNAL, vol. 53, no. 4, December 1998, 25-28.

_____. "Crucial Network Imperatives Spawn Information War Peril." SIGNAL Information Warfare Series, n.d., 4-6.

_____. "Intelligence Agency Adjusts As Mission Possible Unfolds." SIGNAL, vol. 53, no. 2, October 1998, 17-19.

_____. "Redundancy, Robustness Protect Vital National Information Links." SIGNAL Information Warfare Series, n.d., 1-3.

Roberts, Ross. "Desert Fox: The Third Night." U.S. Naval Institute Proceedings, vol. 125/4/1,154, April 1999, 36-40.

- Ryan, Gen Michael. U.S. Air Force Chief of Staff. Interview by Bryan Bender, published in Janes Defense Weekly, vol. 30, no. 18, 4 November 1998, 32.
- Scott, William B. "USAF's EFX '98 Trial to Move Information, Not People." Aviation Week & Space Technology, vol. 148, no. 19, 11 May 1998, 78-79.
- Seigle, Greg. "Air-operations concept promises clearer picture of future warfare." Janes Defense Weekly, vol. 30, no. 13, 30 September 1998, 37-38.
- Shelton, General Henry H. "Operationalizing Joint Vision 2010." Airpower Journal, vol. XII, no. 3, Fall 1998, 102-107.
- Tilelli, Gen John H., Jr. "Ulchi-Focus Lens '97: Putting JV 2010 into Practice." Joint Force Quarterly, no. 17, Autumn-Winter 1997-1998. 76-80.
- Tirpak, John A. "The Chief Holds Course." Air Force Magazine, January 1998, 37-40.
- _____. "Complications Overhead." Air Force Magazine, April 1998, 22-28.
- _____. "The Long Reach of On-Call Airpower." Air Force Magazine, vol. 81, no. 12, December 1998, 20-26.
- U.S. Air Force, Air Combat Command (ACC). Air Combat Command Intelligence Support to the JFACC Concept (3rd Edition). Langley AFB, VA, 30 September 1996.
- U.S. Air Force, Air Combat Command (ACC/DISI). Concept of Operations (Draft) for the Distributed Common Ground System. Langley AFB, VA, 18 January 1999.
- U.S. Air Force, Air Combat Command (ACC/DOI). Concept Paper on Selected Command and Control Nodes (Draft). Langley AFB, VA, 15 October 1998.
- _____. Operations Support Center (OSC) Concept of Operations (Draft). Langley AFB, VA, n.d..
- U.S. Air Force, Electronic Systems Center (ESC/TYG). "AF Distributed Common Ground System." Briefing Slides, Presented by Chris Swift, n.d..
- U.S. Army-Air Force Center for Low-Intensity Conflict. Disaster at Ignalina. Langley AFB, VA, 1 February 1996.
- _____. Tactics, Techniques and Procedures for Humanitarian Assistance Operations in the Former Republic of Yugoslavia. Langley AFB, VA, 15 March 1994.
- U.S. Atlantic Command. USACOM Tactics, Techniques, and Procedures (ATTP) for Intelligence Support to Joint Operations. Norfolk, VA: 20 September 1995.

- _____. Integrated Collection Management Advanced Concept Technology Demonstration. Norfolk, VA: n.d..
<<http://www.eucom.smil.mil/ecj2/j2p/sb/OAS/systems/mditds/adct-icm/adtd-icm.html>> (26 April 1999).
- U.S. Central Command. United States Central Command (USCENTCOM) Concept of Intelligence Operations to Support Operation DESERT FOX. MacDill AFB, FL: 18 December 1998.
- _____. United States Central Command (USCENTCOM) CENTCOM Tactics, Techniques, and Procedures (CTTP) for Intelligence Support to Joint Warfighters. MacDill AFB, FL: 14 August 1998.
- U.S. Congress. House. Armed Services Committee. Hearings before the Armed Services Committee. 106th Congress, 23 February 1999.
- _____. House. Permanent Select Committee on Intelligence. Hearings before the Permanent Select Committee. 106th Congress, 9 March 1999.
- U.S. Department of Defense. Conduct of the Persian Gulf War, Final Report to Congress. Washington, D.C.: April 1992.
- U.S. Forces Korea. Korean Tactics, Techniques, and Procedures. Seoul, Korea: 15 March 1996.
- U.S. Joint Chiefs of Staff. Battlespace Awareness J2 Campaign Plan, Implementing JV2010 (Draft Brief). n.d. <<http://delphi-s.dia.smil.mil/intel/j2/j2p/mainbrf/sldXXX.html>> (11 January 1999)
- _____. C4I for the Warrior Brochure. Washington, D.C.: n.d..
n.d.<<http://cficms.osf.disa.smil.mil:1110/fbsbook/fbsbook.html>> (19 January 1999)
- _____. DOD Dictionary of Military and Associated Terms (Joint Pub 1-02). Washington, D.C.: 23 March 1994.
- _____. Doctrine for Command, Control, Communications, and Computer (C⁴) Systems Support to Joint Operations (Joint Pub 6-0). Washington, D.C.: 30 May 1995.
- _____. Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support For Joint Operations (Joint Pub 3-55). Washington, D.C.: 14 April 1993.
- _____. Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0). Washington, D.C.: 5 May 1995.

- _____. Joint Doctrine, Tactics, Techniques, and Procedures for Counter Intelligence Support to Operations (Joint Pub 2-01.2). Washington, D.C.: 5 April 1994.
- _____. Joint Intelligence Support to Military Operations (Joint Pub 2-01). Washington, D.C.: 20 November 1996.
- _____. Joint Vision 2010. Washington, D.C.: 1996.
- _____. JTTP for Geospatial Information and Services Support for Joint Operations (Draft) (Joint Pub 2-02). Washington, D.C.: n.d..
- _____. JTTP for Intelligence Support to Targeting (Draft) (Joint Pub 2-01.1). Washington, D.C.: n.d..
- _____. JTTP for Joint Intelligence Preparation of Battlespace (Draft) (Joint Pub 2-01.3). Washington, D.C.: n.d..
- _____. National Intelligence Support to Joint Operations (Joint Pub 2-02). Washington, D.C.: 28 September 1998.
- U.S. Joint Chiefs of Staff (JCS/J6). Consolidated Comments and Responses to the 1st Draft of the Information Dissemination Management Mission Need Statement (MSN). 25 September 1998. <www.hq.pacom.smil.mil/j5/req/mns/idm> (19 January 1999)
- _____. Framework for Information Dissemination Management (IDM) Services. 19 Sep 97. <www.hq.pacom.smil.mil/j5/req/mns/idm> (19 January 1999)
- _____. IDM Strategy. 7 Jun 98. <www.hq.pacom.smil.mil/j5/req/mns/idm> (19 January 1999)
- _____. Information Paper: Observations on the Emergence of Network-Centric Warfare. Washington, D.C., n.d.. <<http://www.dtic.mil/jcs/j6/education/warfare.html>> (7 December 1998).
- _____. Mission Need Statement for Information Dissemination Management, 2nd Draft. 23 September 1998. <www.hq.pacom.smil.mil/j5/req/mns/idm> (19 January 1999)
- U.S. Naval Institute and AFCEA. "West '98." Briefing Slides dated 14 January 1998. <<http://www.tci.navy.mil/pma281/briefings/afcea980114/sld 001-032.html>> (12 Feb 99)
- U.S. Secretary of the Air Force. 1998 Air Force Congressional Issue Papers. Washington, D.C.: n.d.. <<http://www.af.mil/lib/afissues/1998/issue98.html>> (January 21, 1999).
- U.S. Strategic Command. U.S. Strategic Command Intelligence Tactics, Techniques, and Procedures for Strategic Operations. Offutt AFB, NE: 25 July 1994.

Wallace, Maj Gen William S., and Lt Col William J. Tait, Jr.. "Intelligence in the Division AWE: A Winner for the Next Millennium." Military Intelligence, vol. 24, no. 2, April-June 1998, 4-8.

Wall, Robert. "Recon Architecture Presages Changes." Aviation Week & Space Technology, vol. 148, no. 20, 18 May 1998, 48-49.

Wentz, Larry. Lessons from Bosnia: the IFOR Experience. Washington, D.C.: National Defense University, 1997.

West, Leslie. "Exploiting the Information Revolution." Sea Power, vol. 41, no. 3, March 1998, 38-40.

Wood, Lt Gen (Ret) C. Norman. "Commercial Technology Companies Find New Defense Opportunities." SIGNAL, vol. 53, no. 4, December 1998, 14.